Titre: Title:	Intrication temporelle et communication quantique
Auteur: Author:	Félix Bussières
Date:	2009
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Bussières, F. (2009). Intrication temporelle et communication quantique [Ph.D. thesis, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/215/

UNIVERSITÉ DE MONTRÉAL

INTRICATION TEMPORELLE ET COMMUNICATION QUANTIQUE

FÉLIX BUSSIÈRES
DÉPARTEMENT DE GÉNIE PHYSIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

THÈSE PRÉSENTÉE EN VUE DE L'OBTENTION DU DIPLÔME DE
PHILOSOPHIÆ DOCTOR
(GÉNIE PHYSIQUE)
OCTOBRE 2009

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Cette thèse intitulée :

INTRICATION TEMPORELLE ET COMMUNICATION QUANTIQUE

présentée par : BUSSIÈRES Félix
en vue de l'obtention du diplôme de : Philosophiæ Doctor
a été dûment acceptée par le jury d'examen constitué de :

M. FRANCŒUR Sébastien, Ph.D., président
M. GODBOUT Nicolas, Ph.D., membre et directeur de recherche
Mme. LACROIX Suzanne, D.Sc., membre et codirectrice de recherche
M. BRASSARD Gilles, Ph.D., membre et codirecteur de recherche
M. TITTEL Wolfgang, Ph.D., membre et codirecteur de recherche
M. MACKENZIE Richard, Ph.D., membre
M. GRANGIER Philippe, Ph.D., membre externe

À Jacynthe.

« *All truths are easy to understand once they are discovered ;*
the point is to discover them. »
– Galilée

Remerciements

Je remercie chaleureusement mes directeurs Nicolas Godbout, Gilles Brassard, Suzanne Lacroix et Wolfgang Tittel. La richesse de votre enseignement sera pour toujours une source d'inspiration.

Les travaux de cette thèse sont le fruit d'un effort commun. Je remercie tous mes co-auteurs : Guido Berlín, Gilles Brassard, José M. Fernandez, Nicolas Godbout, Steve Hosier, Jeongwan Jin, Suzanne Lacroix, Allison Rubenok, Joshua A. Slater, Yasaman Soudagar et Wolfgang Tittel.

Merci à tous mes collègues et amis du *Laboratoire des fibres optiques* de l'École Polytechnique de Montréal, du *Quantum Cryptography and Communication Laboratory* de l'Université de Calgary et du *Laboratoire d'informatique théorique et quantique* de l'Université de Montréal : Maryse Aubé, Guido Berlín, Fanny Béron, Bryan Burgoyne, François Busque, Alexandre Dupuis, Mikäel Leduc, Yannick Lizé, Francis Boismenu, Jérôme Poulin, Sylvain O'reilly, Daniel Summers-Lépine, Yasaman Soudagar, Jürgen Appel, Sean Blancher, Philip Chan, Ahdiyeh Delfan, Eden Figueroa, Chris Healey, Steve Hosier, Gina Howard, Jeongwan Jin, Vladimir Kiselyov, Cecilia La Mela, Itzel Lucio Martinez, Andrew MacRae, Xiaofan Mo, John Nguyen, Allison Rubenok, Hyejeong Hwang, Erhan Saglamyurek, Barry Sanders, Christoph Simon, Neil Sinclair, Joshua A. Slater, Terence Stuart, Hugue Blier, Anne Broadbent, Julien Degorre, Frédéric Dupuis, Olivier Landon-Cardinal, André Méthot, Éric Oliver Paquette, Sébastien Gambs et Alain Tapp.

Je remercie infiniment tous les membres de ma famille et amis qui m'ont encouragé. Je vous aime tous.

Ces travaux ont été supportés financièrement par le Conseil de recherches en sciences naturelles et de génie du Canada (CRSNG), le Fonds québécois de la recherche sur la nature et les technologies (FQRNT), l'Institut canadien pour les innovations en photonique (ICIP) et la Fondation de Polytechnique.

Résumé

La *communication quantique* est l'art de transférer un état quantique d'un endroit à un autre et l'étude des tâches que cela permet d'accomplir. Cette thèse présente des avancées technologiques et théoriques appliquées à la communication quantique dans un contexte réaliste avec essais *sur le terrain*. Ceci a été réalisé à l'aide d'une transmission de l'information quantique par une fibre optique déployée dans un environnement urbain. Les innovations présentées élargissent le champ d'application de l'intrication temporelle à travers l'élaboration de nouvelles méthodes pour manipuler l'encodage temporel, d'un nouveau modèle de caractérisation d'une source de paires de photons, de nouvelles façons d'étudier la non-localité et de l'élaboration et la première réalisation d'un nouveau protocole de pile ou face quantique tolérant aux pertes.

Manipulation de l'encodage temporel

Le photon unique est un excellent véhicule avec lequel un *qubit*, l'unité fondamentale de l'information quantique, peut être encodé. En particulier, l'*encodage temporel* de qubits photoniques est bien adapté à la transmission par fibre optique. Avant les travaux de cette thèse, le champ d'application de cet encodage était limité par l'absence de méthodes réalisant opérations et mesures arbitraires. Nous avons éliminé cette restriction et proposé les premières méthodes permettant de réaliser une opération arbitraire et déterministe sur un qubit temporel ainsi qu'une mesure dans une base arbitraire. Nous avons appliqué ces propositions au cas spécifique du *calcul quantique basé sur la mesure* et sur l'optique linéaire et montré comment réaliser les *opérations en aval* essentielles à cette approche. Ceci ouvre la voie vers la création d'un ordinateur quantique basé sur l'optique, mais également à de nouvelles tâches en communication quantique.

Caractérisation de sources de paires de photons

La communication quantique expérimentale nécessite la création de photons uniques et de paires de photons intriqués. Ces deux ingrédients peuvent être obtenus à partir d'une source de paires de photons basée sur un processus non-linéaire spontané. Plusieurs tâches en communication quantique nécessitent une connaissance précise des propriétés de la source utilisée. Nous avons développé et démontré expérimentalement une nouvelle méthode simple et rapide permettant de caractériser une source de paires de photons. Cette méthode est particulièrement bien adaptée à un contexte de transmission sur le terrain où les conditions expérimentales, telles que la transmittance d'un canal, peuvent fluctuer, et où la caractérisation de la source doit être faite en temps réel.

Non-localité de l'intrication temporelle

L'*intrication* est une ressource permettant la réalisation de plusieurs tâches importantes de la communication quantique. Elle permet aussi de créer des corrélations entre deux systèmes physiques qui ne peuvent être expliquées par la physique classique ; cette manifestation de l'intrication est appelée *non-localité* quantique. Nous avons construit une source d'intrication temporelle et nous l'avons caractérisée à l'aide de mesures à un qubit dans des bases arbitraires. Cela nous a permis de révéler la nature non-locale de notre source d'une manière jamais réalisée auparavant et ouvre la voie à l'étude de nouveaux aspects de la non-localité. Ces expériences ont été réalisées sur le terrain et nous ont permis de vérifier que les corrélations non-locales quantiques ne sont nullement affectées par la transmission d'un des qubits sur 12,4 km de fibre optique souterraine.

Jeux de pile ou face quantique

Le pile ou face quantique est une primitive de la cryptographie quantique proposée en 1984, soit durant les premiers balbutiements de la communication quantique, où deux joueurs s'échangent à tour de rôle de l'information classique et quantique de façon à générer un bit aléatoire commun. L'utilisation de l'information quantique est telle qu'en présence d'un tricheur, ce dernier ne peut biaiser complètement le résultat. Classiquement, ceci est impossible et un des deux joueurs pourra toujours obtenir le résultat désiré en trichant. Malheureusement, la sécurité de tous les protocoles de pile ou face quantique antérieurs est sérieusement compromise en présence de pertes sur le canal de transmission. Nous avons trouvé une solution à ce problème et obtenu le premier protocole de pile ou face quantique *tolérant aux pertes* dont la sécurité est indépendante de la grandeur des pertes. Nous avons ensuite réalisé la première démonstration expérimentale de ce protocole en utilisant notre source d'intrication temporelle combinée aux mesures dans des bases arbitraires que nous avons développées. Cette expérience a été réalisée sur le terrain avec transmission de l'information quantique sur une fibre optique souterraine. Cette nouvelle tâche s'ajoute à la distribution quantique de clés en tant qu'application pratique de la communication quantique.

Mots-clés : communication quantique, photonique, encodage temporel, source de paire de photons, source de photons annoncés, intrication, non-localité, intrication temporelle, intrication hybride, réseau quantique, cryptographie quantique, pile ou face quantique, calcul quantique basé sur la mesure, télécommunication, fibre optique, optique non-linéaire.

Abstract

Quantum communication is the art of transferring a quantum state from one place to another and the study of tasks that can be accomplished with it. This thesis is devoted to the development of tools and tasks for quantum communication in a real-world setting. These were implemented using an underground optical fibre link deployed in an urban environment. The technological and theoretical innovations presented here broaden the range of applications of time-bin entanglement through new methods of manipulating time-bin qubits, a novel model for characterizing sources of photon pairs, new ways of testing non-locality and the design and the first implementation of a new loss-tolerant quantum coin-flipping protocol.

Manipulating time-bin qubits

A single photon is an excellent vehicle in which a *qubit*, the fundamental unit of quantum information, can be encoded. In particular, the *time-bin* encoding of photonic qubits is well suited for optical fibre transmission. Before this thesis, the applications of quantum communication based on the time-bin encoding were limited due to the lack of methods to implement arbitrary operations and measurements. We have removed this restriction by proposing the first methods to realize arbitrary deterministic operations on time-bin qubits as well as single qubit measurements in an arbitrary basis. We applied these propositions to the specific case of optical *measurement-based quantum computing* and showed how to implement the *feedforward operations*, which are essential to this model. This therefore opens new possibilities for creating an optical quantum computer, but also for other quantum communication tasks.

Characterizing sources of photon pairs

Experimental quantum communication requires the creation of single photons and entangled photons. These two ingredients can be obtained from a source of photon pairs based on non-linear spontaneous processes. Several tasks in quantum communication require a precise knowledge of the properties of the source being used. We developed and implemented a fast and simple method to characterize a source of photon pairs. This method is well suited for a realistic setting where experimental conditions, such as channel transmittance, may fluctuate, and for which the characterization of the source has to be done in real time.

Testing the non-locality of time-bin entanglement

Entanglement is a resource needed for the realization of many important tasks in quantum communication. It also allows two physical systems to be correlated in a way that cannot

be explained by classical physics; this manifestation of entanglement is called *non-locality*. We built a source of time-bin entangled photonic qubits and characterized it with the new methods implementing arbitrary single qubit measurements that we developed. This allowed us to reveal the non-local nature of our source of entanglement in ways that were never implemented before. It also opens the door to study previously untested features of non-locality using this source. Theses experiments were performed in a realistic setting where quantum (non-local) correlations were observed even after transmission of one of the entangled qubits over 12.4 km of an underground optical fibre.

Flipping quantum coins

Quantum coin flipping is a quantum cryptographic primitive proposed in 1984, that is when the very first steps of quantum communication were being taken, where two players alternate in sending classical and quantum information in order to generate a shared random bit. The use of quantum information is such that a potential cheater cannot force the outcome to his choice with certainty. Classically, however, one of the players can always deterministically choose the outcome. Unfortunately, the security of all previous quantum coin-flipping protocols is seriously compromised in the presence of losses on the transmission channel, thereby making this task impractical. We found a solution to this problem and obtained the first *loss-tolerant* quantum coin-flipping protocol whose security is independent of the amount of the losses. We have also experimentally demonstrated our loss-tolerant protocol using our source of time-bin entanglement combined with our arbitrary single qubit measurement methods. This experiment took place in a realistic setting where qubits travelled over an underground optical fibre link. This new task thus joins quantum key distribution as a practical application of quantum communication.

Keywords: quantum communication, photonics, time-bin encoding, source of photon pairs, heralded single photon source, entanglement, non-locality, time-bin entanglement, hybrid entanglement, quantum network, quantum cryptography, quantum coin flipping, measurement-based quantum computation, telecommunication, optical fibre, nonlinear optics.

Table des matières

Liste des tableaux

Liste des figures

Liste des sigles et abréviations

MQ	Mécanique quantique	
DQC	Distribution quantique de clés	p. 6
MB	Mesure de Bell	p. 10
KLM	Knill, Laflamme et Milburn	p. 11
ATU	Analyseur temporel universel	p. 25
CQBM	Calcul quantique basé sur la mesure	p. 30
$\|+\rangle$	État $\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	
$\|-\rangle$	État $\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	
$\|+\rangle_\phi$	État $\frac{1}{\sqrt{2}}(\|0\rangle + \mathrm{e}^{i\phi}\|1\rangle)$	
$\|-\rangle_\phi$	État $\frac{1}{\sqrt{2}}(\|0\rangle - \mathrm{e}^{i\phi}\|1\rangle)$	
B_+	Base $B_+ = \{\|0\rangle, \|1\rangle\}$	
$B_\times$	Base $\{\|+\rangle, \|-\rangle\}$	
$B_\times(\phi)$	Base $\{\|+\rangle_\phi, \|-\rangle_\phi\}$	
CPS	Conversion paramétrique spontanée	p. 40
M4O	Mélange à quatre ondes	p. 40
NLPP	Niobate de lithium polé périodiquement	p. 41
μ	Nombre moyen de paires de photons créées (luminosité)	p. 44
EA	Ensemble d'atomes	p. 46
SPA	Source de photons annoncés	p. 49
EPR	Einstein, Podolsky et Rosen	p. 72
CHSH	Clauser, Horne, Shimony et Holt	p. 73
ATVY	Aharonov, Ta-Shma, Vazirani et Yao	p. 99
NFPM	Nguyen, Frison, Huy et Massar	p. 100
Éq.	Équation	
Fig.	Figure	

Chapitre 1

Introduction

Nous vivons dans une *société de l'information* où « [...] la création, la distribution, la communication, l'utilisation et la manipulation de l'information joue un rôle économique, politique et culturel. » [1]. En date du 1er septembre 2009, 24,7% de la population mondiale utilise Internet, soit environ 1,67 milliards d'utilisateurs [2]. Entre 2000 et 2009, ce nombre a augmenté de 362%.

Les technologies de l'information que nous utilisons aujourd'hui puisent souvent leurs fondements dans les idées d'hier. Par exemple, la télécommunication à haut débit est, d'une certaine façon, une version moderne des signaux de fumée anciennement utilisés pour transmettre un message sur quelques kilomètres. La différence entre ces deux méthodes est le substrat, pas la substance. Cette substance est l'information elle-même. La représentation que nous donnons à l'information a, jusqu'à tout récemment, toujours été la même. Cette représentation peut être qualifiée de « classique » lorsqu'on la compare aux lois de la physique classique qui étaient en vigueur à la fin du 19e siècle. Par exemple, en mécanique newtonnienne, la position d'une particule est donnée par le vecteur position $\mathbf{r}$. Si la particule se déplace et atteint une nouvelle position $\mathbf{r}'$, alors la mesure de cette position produira, bien entendu, le résultat $\mathbf{r}'$. De la même façon, un bit d'information est soit dans l'état « 0 », soit dans l'état « 1 », et la mesure de cet état nous permet de le révéler.

Au début du 20e siècle, la physique a vécu un changement de paradigme avec l'arrivée de la mécanique quantique (MQ). Cette théorie a forcé les physiciens à modifier fondamentalement la description de la nature qu'ils s'étaient donné. Selon cette nouvelle description, un système physique peut se trouver en superposition de deux ou plusieurs états « classiques », et la mesure de ce système peut perturber cet état. Ce principe de superposition permet également de préparer deux ou plusieurs systèmes dans un état *intriqué*. Comme nous le verrons, l'intrication est une propriété de la MQ qui a des répercussions importantes sur les corrélations entre deux systèmes.

Au cours des vingt-cinq dernières années, notre représentation de l'information a elle aussi vécue un changement de paradigme. L'information peut maintenant être considérée comme « quantique ». La beauté de cette généralisation ne serait cependant qu'éphémère et sans intérêt si ses conséquences n'étaient qu'esthétiques. Or, c'est tout le contraire. En 1984,

Charles H. Bennett et Gilles Brassard ont montré que l'information quantique, lorsqu'elle est utilisée à des fins de cryptographie, a un avantage substantiel et pratique par rapport à l'information classique [3]. De la même façon, le calcul basé sur l'information quantique a lui aussi montré qu'un ordinateur quantique pourrait résoudre des problèmes insurmontables par un ordinateur classique [4]. Ainsi, l'information quantique permet de réaliser certaines tâches qui sont autrement impossibles à réaliser avec seulement de l'information classique !

Cette thèse porte sur la *communication quantique*. Cette discipline peut être définie comme l'art de transférer un état quantique d'un endroit à un autre et l'étude des tâches que cela permet d'accomplir. D'un point de vue expérimental, la communication quantique s'est considérablement développée au cours des quinze dernières années. Ce développement a maintenant atteint la sphère commerciale [5, 6, 7]. Ce succès est en grande partie lié au fait que la lumière est le véhicule idéal pour transférer de l'information quantique.

Dans ce chapitre, nous présentons d'abord quelques propriétés de l'information quantique qui la distinguent de l'information classique. Ensuite, nous discutons des implications que la mécanique quantique, plus particulièrement l'intrication, a sur les corrélations possibles entre systèmes physiques. Nous présentons ensuite quelques tâches importantes de la communication quantique et du calcul quantique et nous verrons que l'intrication peut être considérée comme une ressource. Nous concluons avec un résumé des contributions de cette thèse.

Les références [8, 9, 10] présentent une revue de plusieurs aspects importants de la communication quantique. Quelques ouvrages d'introduction au domaine du traitement de l'information quantique sont disponibles, notamment les références [4] et [11].

1.1 Information quantique

Le *bit classique*, ou *bit*, est une unité d'*information classique* [12]. Plus précisément, un bit b est une abstraction d'un système physique dont l'ensemble des états possibles (qui sont mutuellement exclusifs) est binaire : $b \in \{0, 1\}$. Par exemple, considérons un laser générant de la lumière couplée dans une fibre optique (utilisée comme canal de transmission) et dont l'intensité peut être modulée dans le temps. Un $\ll 0 \gg$ peut être transmis en envoyant rien du tout, tandis qu'un $\ll 1 \gg$ peut être transmis par une impulsion dont l'intensité est au-delà d'un certain seuil de décision. La télécommunication actuellement utilisée sur le réseau Internet est fondée sur ce paradigme.

Le *bit quantique*, ou *qubit*, est une abstraction d'un système quantique dont une observable possède deux états propres, notés $|0\rangle$ et $|1\rangle$, formant une base orthonormée $\mathcal{B}_+ = \{|0\rangle, |1\rangle\}$. Les propriétés d'un qubit découlent des postulats de la mécanique quantique [4, 13]. Par conséquent, l'état d'un qubit correspond à un vecteur d'état dans un espace de Hilbert

complexe à deux dimensions :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.1}$$

où les coefficients complexes α et β respectent la condition de normalisation : $|\alpha|^2 + |\beta|^2 = 1$. Un qubit, contrairement à un bit, peut donc se trouver en *superposition* de ses états propres. Il constitue une unité d'*information quantique* et est une généralisation de l'information binaire classique. En posant $\alpha = \cos\frac{\theta}{2}$ et $\beta = \mathrm{e}^{i\varphi}\sin\frac{\theta}{2}$, l'état $|\psi\rangle$ peut être représenté sur la *sphère de Bloch* à l'aide d'un vecteur unitaire faisant un angle θ avec l'axe z et un angle azimutal φ avec l'axe x, tel qu'illustré sur la fig. 1.1 [4].

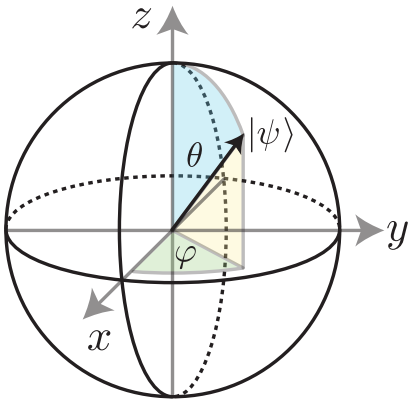

FIGURE 1.1 État $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ représenté par un vecteur unitaire sur la sphère de Bloch.

L'information quantique est plus fragile que l'information classique. Ceci devient évident lorsqu'on applique le postulat de la mesure à un qubit. En effet, la *mesure projective* de l'état $|\psi\rangle$ dans la base $\mathcal{B}_+$ produira le résultat $|0\rangle$ avec la probabilité $|\alpha|^2$ ou le résultat $|1\rangle$ avec une probabilité à $|\beta|^2$, et l'état suivant la mesure est *projeté* sur le résultat obtenu. À moins que l'état initial ne corresponde à un des états de la base de mesure,[1] l'état est *perturbé* par la mesure. Cette évolution probabiliste (et irréversible lorsque l'état initial était inconnu) est parfois appelée *effondrement du paquet d'onde*.

La superposition quantique a une étrange et remarquable conséquence lorsqu'on considère un système composé de plusieurs sous-systèmes : elle permet l'existence d'un état qui ne peut être décrit comme la somme des descriptions de chaque sous-système. Par exemple, l'état

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \tag{1.2}$$

1. Dans ce cas, le qubit est équivalent à un bit classique et la mesure de ce dernier ne perturbera pas son état.

décrivant l'état conjoint de deux qubits intriqués, ne peut être factorisé en un produit tensoriel de deux états distincts : $|\Phi^+\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$, où $|\psi_1\rangle$ et $|\psi_1\rangle$ s'écrivent comme l'éq. 1.1. On dit alors que les deux qubits sont dans un état *intriqué*, ou tout simplement qu'ils sont intriqués. L'intrication est une ressource quantique jouant un rôle essentiel dans plusieurs applications de la communication quantique et du calcul quantique, ainsi que le présentent les sections suivantes.

Une autre propriété frappante de l'information quantique est le *théorème de non-clonage* [14, 15, 16]. Les postulats de la mécanique quantique sont tels qu'une « machine » capable de cloner un qubit dans un état inconnu ne peut exister. Le contraste entre l'information classique et quantique est énorme car la possibilité de copier l'information classique, inconnue ou pas, est essentielle au bon fonctionnement de tous nos systèmes de traitement de l'information, du téléphone à l'ordinateur.

1.2 Qubits photoniques

La lumière est un choix naturel pour encoder de l'information quantique, particulièrement lorsque la nature de la tâche nécessite une transmission sur une longue distance. Elle possède plusieurs degrés de liberté permettant d'encoder et de traiter de l'information quantique. Dans le cadre de cette thèse, nous ne considérons que l'encodage en polarisation et l'encodage temporel (définis ci-dessous). D'autre types d'encodage existent et le lecteur est invité à consulter les références [8] et [17] pour plus d'information.

La génération d'un photon unique peut se faire de façon approximative à l'aide d'une impulsion laser fortement atténuée, ou encore à partir d'une source de paires de photons basée sur un processus non-linéaire spontané (cf. section 3). Le qubit peut être encodé dans un des degrés de liberté de ce photon. La polarisation, par exemple, peut être décrite à l'aide d'une superposition des états horizontal et vertical, $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$, où $\{|H\rangle, |V\rangle\}$ constitue une base orthonormée. La création d'un qubit de polarisation dans un état arbitraire est obtenue avec une lame demi-d'onde placée entre deux lames quart d'onde. La mesure dans une base arbitraire est obtenue avec une lame quart d'onde suivie d'une lame demi-onde et d'un cube polarisant. Un autre exemple, qui sera défini formellement au chapitre 2, est l'*encodage temporel*[2] [18]. Un qubit temporel est représenté par un photon en superposition de présence à l'intérieur de deux fenêtres temporelles de durée τ et centrées aux temps t_0 et t_1, $|\psi\rangle = \alpha|t_0\rangle + \beta|t_1\rangle$, où $\Delta t = t_1 - t_0 \gg \tau$. Ces fenêtres sont mutuellement exclusives et forment une base orthonormée que l'on note $\{|t_0\rangle, |t_1\rangle\}$. La manipulation de l'encodage temporel est discutée au chapitre 2.

2. « Time-bin encoding ».

L'intrication photonique nécessite deux ingrédients : le premier est une source de paires de photons et le deuxième est une méthode pour intriquer les photons de chaque paire. Une source probabiliste de paires de photons peut être réalisée, entre autres, en pompant un milieu non-linéaire avec un laser de façon à créer des paires à l'aide de la conversion paramétrique spontanée (CPS) ou le mélange à quatre ondes (M4O) spontané (cf. chapitre 3). Des méthodes permettant d'obtenir une source d'intrication en polarisation à partir de la CPS ou le M4O sont présentées au chapitre 4. Ces méthodes, développées vers la fin des années 90 [19, 20, 18], sont maintenant très répandues. En 1999, elles ont été adaptées pour créer de l'intrication temporelle [18].

1.3 Intrication et non-localité

La mécanique quantique semble défier l'intuition. Cela est mis en évidence en considérant les corrélations entre les résultats des mesures faites sur deux qubits préparés dans l'état intriqué $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Par exemple, supposons que deux observateurs, Alice et Bob, possèdent chacun un qubit de l'état $|\Psi^-\rangle$. La MQ prédit que si Alice et Bob appliquent tous les deux la même transformation arbitraire $\hat{U}$ sur leur qubit respectif[3] avant de le mesurer dans la base $\mathcal{B}_+ = \{|0\rangle, |1\rangle\}$, leurs résultats seront aléatoires mais opposés, indépendamment de la transformation qu'ils ont appliquée, de la distance qui les sépare et de qui a mesuré le premier. La MQ n'explique pas l'origine de ces corrélations, elle ne fait que donner la recette pour prédire les résultats. En particulier, elle doit invoquer l'effondrement du paquet d'onde. Celui-ci peut sembler en contradiction avec la relativité restreinte si on suppose qu'il constitue réellement une influence physique (et potentiellement instantanée) entre le premier qubit et le deuxième.

En 1935, A. Einstein, N. Podolsky et N. Rosen (EPR), alors insatisfaits de la MQ, ont écrit un article célèbre dans lequel ils ont émis l'hypothèse que la MQ est une description incomplète de la réalité physique [21]. Selon EPR, la MQ doit être complétée par l'ajout de *variables locales cachées*, c'est-à-dire inconnues et potentiellement inaccessibles, permettant de redonner à la MQ un caractère plus « réaliste ». En particulier, cet ajout serait tel qu'une mesure faite sur une particule ne peut que révéler son état et non pas le perturber. Ceci permettrait alors d'éviter tout recours à l'effondrement du paquet d'onde (et potentiellement à une influence instantanée) pour expliquer l'origine des corrélations issues de l'intrication.

La question de l'existence des variables locales cachées et de leur nécessité demeura en suspens jusqu'en 1964 lorsque J. S. Bell découvrit qu'elle pouvait être testée expérimentalement [22]. Le scénario de Bell, inspiré par les travaux de D. Bohm et Y. Aharonov [23], met en

3. Cette transformation correspond à une rotation sur la sphère de Bloch [4].

scène une source émettant des paires de qubits dans des directions opposées vers Alice et Bob, tel qu'illustré sur la fig. 1.2-a. Chaque qubit est mesuré dans une base choisie au hasard entre deux possibilités. En supposant que le choix d'Alice ne peut influencer le résultat obtenu par Bob et vice versa, ce qui constitue l'hypothèse de la *localité*, J. S. Bell montra que les corrélations prédites par une théorie à variables locales cachées sont contraintes par certaines inégalités, aujourd'hui nommées *inégalités de Bell*. En particulier, l'inégalité de Bell-CHSH prédit la borne $S \leq 2$, où S est un paramètre expérimental calculé à partir des corrélations observées [24]. Or, si on suppose que la source émet des qubits intriqués dans l'état $|\Psi^-\rangle$, les corrélations prédites par la MQ donnent $S \leq 2\sqrt{2}$. La conclusion est qu'une théorie à variables cachées ne peut reproduire toutes les prédictions de la MQ et que cette dernière est une théorie *non-locale* [22].

Les premières violations de l'inégalité de Bell-CHSH, utilisant toutes l'intrication en polarisation, trouvèrent que la nature est non-locale [25, 26, 27, 28, 29]. Le constat fut le même lorsque l'expérience fut répétée avec l'intrication temporelle [30, 31] et pour une distance de 10 km séparant Alice et Bob [32, 33]. Une description historique est présentée dans la référence [8].

La non-localité est un champ d'étude très vaste et plusieurs variantes ont été étudiées, notamment les théories non-locales contraintes [34, 35], la non-localité à trois joueurs [36], la non-localité avec qudits [37, 38] et la *pseudo-télépathie quantique* [39, 40]. Une liste exhaustive serait trop longue pour être présentée ici. Il est à noter que toutes les expériences testant la non-localité dans un scénario autre que celui de l'inégalité de Bell-CHSH ont utilisé l'intrication en polarisation. Avec l'intrication temporelle, seule l'inégalité de Bell-CHSH a été testée.

1.4 Cryptographie quantique

La première application concrète de l'information quantique fut en cryptographie. La cryptographie est l'étude et la pratique de la confidentialité, de l'authenticité et de l'intégrité de l'information [41]. Nous présentons ici deux sujets de recherche actuels dans le domaine de la cryptographie quantique.

1.4.1 Distribution quantique de clés

Supposons qu'Alice désire envoyer un message confidentiel à Bob en utilisant un canal public. Ce canal peut être lu par n'importe qui, y compris une espionne habituellement nommée Ève. Cette communication entre Alice et Bob ne peut être réalisée avec une *sécurité incondi-*

tionnelle[4] que si Alice et Bob partagent une chaîne de bits aléatoires secrète, qu'on appelle *clé cryptographique*, et qui doit être aussi longue que le message et inconnue d'Ève [42]. Alice et Bob doivent trouver un moyen de distribuer cette clé entre eux sans qu'un espion puisse en prendre connaissance. Une solution est de forcer Alice et Bob à se rencontrer en personne pour échanger la clé, mais cela n'est malheureusement pas très pratique sur un réseau tel que l'Internet. Une autre option est d'utiliser la *cryptographie à clé publique* [42] avec laquelle Alice chiffre une clé et l'envoie à Bob. La sécurité de ce type de chiffrement est basée sur l'hypothèse que certaines fonctions mathématiques sont faciles à calculer mais très « difficiles » à inverser. Cette difficulté peut être quantifiée en termes du temps de calcul nécessaire pour inverser la fonction avec le meilleur algorithme connu et une puissance de calcul donnée. Cette sécurité repose donc sur des hypothèses calculatoires. Généralement, aucune preuve de ces hypothèses n'existe. En particulier, la sécurité du chiffrement RSA [43], inventé en 1978 et maintenant utilisé à grande échelle sur l'Internet, n'a toujours pas été prouvée. Une autre menace, potentiellement pire, plane également sur la sécurité du chiffrement RSA, celle de l'ordinateur quantique, tel que discuté à la section 1.6.

Vers la fin des années 70, S. Wiesner montra comment la mécanique quantique permet, en principe, de créer des billets de banque impossibles à contrefaire [44]. Puis, en 1984, C. H. Bennett et G. Brassard ont appliqué des idées similaires au problème de la distribution de clé [3]. Plus particulièrement, ils ont inventé un protocole de *distribution quantique de clés*[5] (DQC) où Alice envoie à Bob des qubits dont les états sont choisis aléatoirement parmi ceux de la base $\mathcal{B}_+ = \{|0\rangle, |1\rangle\}$ ou ceux de la base $\mathcal{B}_\times = \{|+\rangle, |-\rangle\}$, où $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Bob mesure ensuite ces qubits dans la base $\mathcal{B}_+$ ou $\mathcal{B}_\times$, choisie au hasard pour chaque qubit. À chaque fois que les bases de préparation et de mesure sont les mêmes, le résultat de la mesure de Bob correspond à l'état qu'Alice à envoyé. Lorsque ces bases diffèrent, le résultat de Bob est aléatoire. Ils peuvent donc générer une clé cryptographique aléatoire en sélectionnant *a posteriori* les cas où la préparation et la mesure ont eu lieu dans la même base. Cette phase de réconciliation des bases est faite sur le canal public et ne compromet pas la sécurité de la clé.[6] En raison de l'impossibilité de discerner des états non orthogonaux sans encourir une probabilité non nulle de perturber ces états, toute tentative par Ève d'extraire de l'information sur la clé finale cause inévitablement des erreurs entre la clé d'Alice et celle de Bob. En fait, la quantité d'information obtenue par Ève peut être déduite directement du taux d'erreur sur la clé. Ces erreurs peuvent ensuite être éliminées

4. La sécurité est inconditionnelle lorsqu'elle peut être prouvée formellement à l'aide de la théorie de l'information de Shannon [42].

5. « Quantum key distribution ».

6. En pratique, tous les messages échangés sur le canal public doivent être authentifiés [45, 46]. Ceci nécessite qu'Alice et Bob partagent une clé avant de débuter la DQC. Ainsi, la DQC est une primitive permettant de créer une clé arbitrairement longue à partir d'une clé de longueur finie.

grâce à la *correction d'erreur* et l'information de l'espion peut être réduite à zéro grâce à la *distillation de la confidentialité*[7] [47, 48]. Le protocole de C. H. Bennett et G. Brassard est aujourd'hui nommé *protocole BB84*.

Une revue de la DQC est présentée dans les références [9] et [49]. La DQC est une technologie disponible commercialement [5, 6, 7].

1.4.2 Pile ou face quantique

La cryptographie s'intéresse également aux tâches où Alice et Bob sont potentiellement des adversaires. Une de ces tâches est le jeu de *pile ou face*. Supposons qu'Alice et Bob désirent tirer à pile ou face au téléphone mais ne se font pas confiance [50]. On aimerait trouver un protocole où Alice et Bob s'échangent de l'information à tour de rôle dans le but de produire un résultat correspondant à un bit aléatoire non biaisé malgré la présence potentielle d'un tricheur. Classiquement, ceci est impossible à réaliser avec une sécurité inconditionnelle : un des participants doté d'une puissance de calcul illimitée aura toujours la possibilité de biaiser complètement le résultat en trichant. L'utilisation de l'information quantique serait-elle la solution ? La question à été posée par C. H. Bennett et G. Brassard dans le même article où la DQC a été proposée [3]. La réponse à cette question est affirmative mais un certain biais est inévitable [51, 52, 53]. Le jeu de *pile ou face quantique* est un domaine de recherche actif et plusieurs protocoles ont été proposés (cf. chapitre 5). Malheureusement, la sécurité de tous ces protocoles est sérieusement compromise en présence d'imperfections telles que le bruit et les pertes sur le canal [54]. Ces aspects sont discutés en détail au chapitre 5.

1.5 Communication quantique et intrication

En communication quantique, l'intrication est considérée comme une *ressource* permettant d'accomplir plusieurs tâches. Nous en présentons quelques unes.

Distribution quantique de clés avec intrication

La première application concrète de l'intrication fut la distribution quantique de clés. En 1991, A. Ekert découvrit qu'en utilisant le montage de la fig. 1.2-a, Alice et Bob peuvent tirer profit des corrélations issues de l'intrication quantique pour générer une clé cryptographique partagée, inconnue de l'espion. Le protocole de A. Ekert est tel que toute tentative par un espion d'extraire de l'information sur la clé générée affecte les corrélations et que la présence de l'espion est révélée à l'aide d'un test d'une inégalité de Bell [55]. En 1992, C. H. Bennett,

7. « Privacy amplification ».

G. Brassard et N. D. Mermin montrèrent que le protocole BB84 peut être réalisé à l'aide de l'intrication et que l'utilisation d'une inégalité de Bell n'est pas nécessaire pour révéler la présence de l'espion [56]. Ces deux approches ont été démontrées pour la première fois en 2000 par trois groupes utilisant soit l'intrication en polarisation avec transmission à l'air libre [57, 58], soit l'intrication temporelle avec transmission sur fibre optique [59].

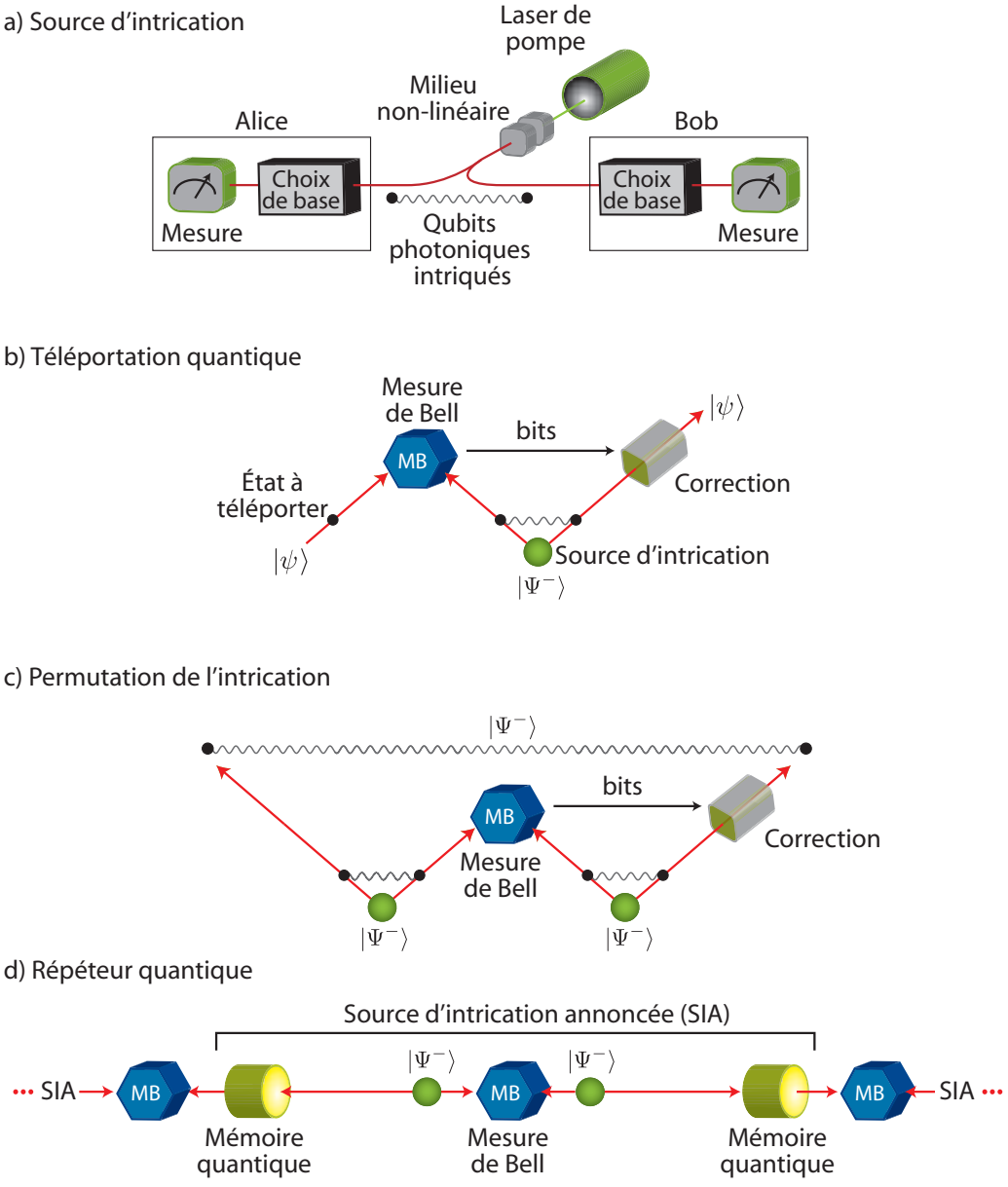

FIGURE 1.2 Communication quantique basée sur l'intrication.

Téléportation quantique

L'intrication permet de téléporter un qubit dans un état inconnu [60]. Supposons qu'Alice et Bob partagent une paire de qubits intriqués dans l'état $|\Psi^-\rangle$ et qu'Alice possède un qubit dans un état inconnu $|\psi\rangle$ qu'elle désire envoyer à Bob (cf. fig. 1.2). Pour ce faire, elle applique une mesure de Bell [8] sur le système conjoint formé par le qubit à envoyer et sa moitié de la paire intriquée. La mesure de Bell a pour effet de téléporter, à une correction unitaire près, l'état $|\psi\rangle$ sur l'autre qubit de la paire intriquée. Cette correction dépend du résultat de la mesure de Bell et son application nécessite la transmission de deux bits classiques. La téléportation d'un qubit de polarisation a été démontrée pour la première fois en 1997 [61] et répétée avec une mesure de Bell complète en 1998 [62]. Elle a aussi été réalisée sur une distance de 50 m avec l'intrication temporelle et transmission par fibre optique [63].

Permutation de l'intrication

Le concept de la téléportation quantique permet d'aller plus loin que la téléportation d'un qubit. En effet, l'intrication elle-même peut être téléportée [64]. Considérons le montage de la fig. 1.2-c où un qubit d'une paire intriquée dans l'état $|\Psi^-\rangle$ est téléporté. Les deux qubits restants après la mesure de Bell sont intriqués même s'ils n'ont jamais interagi directement. Cette *permutation de l'intrication* a été démontrée à l'aide de l'encodage en polarisation en 1998 [65] et améliorée en 2002 de façon à violer l'inégalité de Bell-CHSH [66]. Elle a également été démontrée avec l'intrication temporelle en 2005 [67].

Répéteur quantique

Le transfert d'un état quantique sur une longue distance est essentiel au développement futur de la communication quantique, en particulier de la DQC. En pratique, la distance est fondamentalement limitée par les pertes car l'amplification optique de l'information quantique est impossible en raison du théorème de non-clonage. Une solution possible pour surmonter cette barrière est de réaliser un *répéteur quantique* [68]. L'idée de base derrière le répéteur quantique vient du fait que la permutation d'intrication peut, en principe, être répétée un nombre arbitraire de fois afin d'établir une paire intriquée sur une distance arbitrairement grande. Ceci n'est cependant pas suffisant pour surmonter les pertes car la probabilité que tous les photons se rendent aux jonctions est égale à la probabilité qu'un seul photon parcoure tout le lien. Pour remédier à ce problème, on peut créer une source d'intrication annoncée

8. La *base de Bell* est la base définie par les quatre *états de Bell* $|\Phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ et $|\Psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$. Une *mesure de Bell* (MB) est une mesure projetant deux qubits sur un des états de Bell. Une MB incomplète, projetant sur un sous ensemble des quatre états, peut être réalisée avec une probabilité de réussite d'au plus 50% avec l'optique linéaire seulement [8].

(SIA) composée de deux sources d'intrication concaténées par une mesure de Bell et de deux mémoires quantiques, tel qu'illustré à la fig. 1.2-d. Lorsque la mesure de Bell a réussi, elle annonce que les mémoires stockent des photons intriqués (avec une certaine probabilité). Ceci permet d'attendre que les sources voisines aient également stocké des photons avant de les relâcher pour réaliser la mesure de Bell. La réalisation d'une mémoire quantique efficace est un domaine recherche qui est présentement en ébullition. L'approche ayant jusqu'à maintenant eu le plus de succès consiste à stocker les photons dans la superposition cohérente d'un ensemble d'atomes [69, 70, 71].

1.6 Calcul quantique

Pour une introduction au calcul quantique, consulter les références [4] et [72].

La possibilité de simuler un système quantique en utilisant un ordinateur où l'information est traitée de façon quantique a d'abord été envisagée par R. Feynman en 1982 [73]. Puis, la première description d'un ordinateur quantique universel fut présentée par D. Deutsch en 1985 [74]. La puissance de calcul offerte par un ordinateur quantique devint évidente lorsque, en 1994, P. Shor montra qu'un ordinateur quantique peut résoudre efficacement le problème de la factorisation sur lequel la sécurité du chiffrement RSA est basée [75]. Un autre exemple important est celui de la recherche dans une liste non triée. En 1995, L. Grover montra qu'un ordinateur quantique pourrait trouver un élément donné avec $\mathcal{O}(\sqrt{n})$ requêtes à la liste, où n est la taille de la liste, comparativement à $\mathcal{O}(n)$ requêtes pour le meilleur algorithme classique [76]. Ces exemples illustrent le fait qu'un ordinateur quantique offre, pour certains problèmes, une puissance de calcul grandement supérieure à celle d'un ordinateur classique.

Un ordinateur quantique peut être modélisé comme un ensemble de qubits sur lesquels on applique une séquence des portes quantiques implémentant l'algorithme. Le calcul se termine par la mesure d'un sous-ensemble de qubits contenant le résultat. Ce modèle requiert un ensemble universel de portes quantiques contenant au moins une porte à plusieurs qubits, c'est-à-dire une porte permettant de mettre en interaction deux ou plusieurs qubits.

La réalisation de portes à plusieurs qubits représente un défi technologique de grande envergure. En optique, l'efficacité des interactions non-linéaires est si faible que deux photons uniques n'interagissent pratiquement pas entre eux. La réalisation d'une porte à deux qubits basée sur cette approche est présentement hors de portée. Une autre approche a été proposée par E. Knill, R. Laflamme et G. Milburn (KLM) [77]. Ils ont montré qu'en combinant sources de photons uniques, détecteurs capables de résoudre le nombre de photons et composants optiques linéaires, il est possible de réaliser efficacement une porte à deux qubits et d'obtenir un ensemble universel de portes quantiques. Cette contribution est conceptuellement très

importante mais sa réalisation à grande échelle est hors de la portée de la technologie actuelle.

En 2001, un modèle appelé *calcul quantique basé sur la mesure* a été proposé [78, 79]. Dans cette approche, la difficulté technologique est déplacée vers la génération d'un type particulier d'état nommé « cluster » où plusieurs qubits sont intriqués mutuellement selon certaines règles. L'intérêt de ce modèle provient du fait que le traitement correspond à mesurer les qubits du « cluster » dans un ordre pré-déterminé par l'algorithme et d'appliquer des opérations à un qubit avant de les mesurer. Les opérations à appliquer dépendent des résultats des mesures antérieures.[9] Le modèle du calcul quantique basé sur la mesure a permis de réaliser plusieurs démonstrations de principe à l'aide d'un registre de quelques qubits photoniques [80, 81, 82, 83, 84].

1.7 Contributions de cette thèse

Les contributions scientifiques de cette thèse sont résumées ci-dessous. Les résumés sont accompagnés de la liste des publications associées à ces travaux. Parmi toutes les présentations orales données sur ces travaux, seules celles qui ont été données par l'auteur de cette thèse sont énumérées.

Manipulation de l'encodage temporel (chapitre 2)

Problématique

L'encodage temporel [18] de qubits photoniques possède deux propriétés intéressantes pour la communication quantique. Premièrement, il est intrinsèquement insensible à la biréfringence lors de sa transmission par fibre optique. Deuxièmement, cet encodage permet, contrairement à l'encodage en polarisation, de générer des *qudits* correspondant à la généralisation d'un qubit à $d > 2$ dimensions [8]. Une limitation importante de l'encodage temporel est que les opérations unitaires et déterministes sur un qubit, tout comme une mesure déterministe dans une base arbitraire, ne sont pas triviales à réaliser en pratique. Une façon de contourner ce problème est de remplacer l'opération (ou la mesure) déterministe par une opération (mesure) non-déterministe, c'est-à-dire ayant une probabilité de réussite inférieure à 100%, mais qui est plus facile à réaliser en pratique. Ceci réduit inévitablement la probabilité de succès de la tâche. Par exemple, la téléportation d'un qubit temporel ne peut être réalisée de façon déterministe sans l'application d'une opération à un qubit pour corriger l'état téléporté [63, 67]. De la même façon, le calcul quantique basé sur l'optique linéaire nécessite des opérations en aval déterministes sans lesquelles il ne pourra être réalisé avec un

9. Ce type d'opération est nommé *opération en aval* (« Feedforward operation »).

grand nombre de qubits.

Contributions

Dans la première partie de ce chapitre, nous proposons deux méthodes permettant d'implémenter une opération unitaire, arbitraire et déterministe sur un qubit temporel à l'aide de composants optiques tout-fibre. Nous montrons aussi comment utiliser ces méthodes pour mesurer un qubit temporel dans une base arbitraire. Une généralisation au cas d'un *qudit* temporel est ensuite présentée. Une construction explicite nécessitant $\mathcal{O}(d^2)$ coupleurs 2×2 et d modulateurs de phase est donnée, où d est la dimension du qudit. Une discussion sur la faisabilité des méthodes est présentée. Ce travail vise à éliminer certaines limitations généralement associées à la manipulation de l'encodage temporel dans le but de le rendre plus polyvalent et applicable à des tâches nécessitant des opérations arbitraires.

Publications associées

• F. Bussières, Y. Soudagar, G. Berlín, S. Lacroix et N. Godbout, « Manipulating time-bin qubits with fiber optics components », *Digest of the IEEE/LEOS Summer Topical Meetings*, pp. 22–23, 2006.

• F. Bussières, Y. Soudagar, G. Berlín, S. Lacroix et N. Godbout, « Deterministic unitary operations on time-bin qudits for quantum communication ».
`arXiv:quant-ph/0608183`, 2006.

Dans la deuxième partie de ce chapitre, nous proposons une architecture tout-fibre du calcul quantique basé sur la mesure permettant de réaliser les *opérations en aval* essentielles à cette approche. Cette implémentation est basée sur l'encodage temporel de qubits. Pour créer les états intriqués à plusieurs qubits, nous utilisons les résultats de D. E. Browne et T. Rudolph [85] qui montrent comment créer un état « cluster » avec l'optique linéaire. Nous appliquons ensuite les méthodes présentées dans la première partie de ce chapitre pour obtenir une architecture tout-fibre permettant, en principe, de créer un « cluster » arbitraire. Nous montrons finalement comment les opérations en aval peuvent être réalisées en utilisant des composants tout-fibre. Nous croyons que cette approche permettra de réduire substantiellement le temps nécessaire pour « programmer » ces opérations en comparaison avec ce qui a été réalisé jusqu'ici. Nous croyons également que le guidage spatial offert par la fibre optique permettra d'éliminer certains problèmes inhérents à la transmission à l'air libre.

Publication associée

• Y. Soudagar, F. Bussières, G. Berlín, S. Lacroix, J. M. Fernandez et N. Godbout, « Cluster state quantum computing in optical fibers », *Journal of the Optical Society of America B*, vol. 24, no. 2, pp. 226–230, 2006.

Sources de paires de photons (chapitre 3)

Problématique

Les sources de paires de photons sont un élément essentiel à la réalisation de plusieurs tâches en communication quantique. Plusieurs de ces tâches, comme la distribution quantique de clés basée sur l'intrication ou sur une source de photons annoncés, bénéficient grandement de la connaissance de la *luminosité* de la source, définie comme le nombre moyen de paires émises par unité de temps. L'estimation de la luminosité d'une source de paires de photons est une tâche non triviale lorsque la transmittance des canaux de transmission est inconnue. De plus, la mesure de ces transmittances est généralement difficile à réaliser lorsque la luminosité est très faible. Par conséquent, une méthode simple, rapide et précise permettant d'estimer la luminosité d'une source ainsi que la transmittance de chaque canal est nécessaire.

Contributions

Nous présentons un modèle décrivant les statistiques des coups d'une source probabiliste de paires de photons. À l'aide de ce modèle, une méthode simple et rapide permettant d'estimer la luminosité de la source ainsi que la transmittance des canaux de transmission est dérivée. Cette méthode est appliquée à une source basée sur la conversion paramétrique spontanée dans un cristal de niobate de lithium ($LiNbO_3$) « polé » périodiquement et produisant des paires de photons à 812 et 1532 nm. La validité et la précision de notre modèle est démontrée en comparant la prédiction et la mesure directe de l'autocorrélation de second ordre $g^{(2)}(0)$ d'une source de photons annoncés. Notre méthode est utile lorsque la luminosité de la source doit être ajustée rapidement et sur demande. Ceci est particulièrement intéressant pour plusieurs applications en communication quantique telles que la DQC basée sur une source photons annoncés ou sur une source d'intrication, ou encore pour optimiser la distance et le taux d'erreur d'un répéteur quantique, tout cela dans un contexte où les conditions expérimentales, comme la transmittance d'un canal, peuvent fluctuer rapidement.

Publication associée

• F. Bussières, J. A. Slater, N. Godbout et W. Tittel, « Fast and simple characterization of a photon pair source », *Optics Express*, vol. 16, no. 21, pp. 17060–17069, 2008.

Intrication temporelle et non-localité (chapitre 4)

Problématique

La problématique derrière les travaux présentés dans ce chapitre est double.

1. L'intrication temporelle a permis de réaliser plusieurs tâches importantes de la communication quantique et de montrer que ces tâches peuvent être réalisées dans le contexte

réel d'un réseau de fibre optique [8, 9, 63, 67]. Malgré ces progrès énormes, cette utilisation était, jusqu'ici, limitée à des tâches nécessitant la projection des qubits sur des états situés soit sur l'équateur de la sphère de Bloch, soit sur les pôles. Or, plusieurs tâches nécessitent ou bénéficient grandement de la possibilité de projeter sur des états autres que ceux-ci. Sans la liberté de projeter sur une base arbitraire, le champ d'application de l'intrication temporelle reste limité.

2. L'intrication est un concept indépendant de la réalisation physique qu'il prend. Ainsi, l'intrication entre deux qubits photoniques devrait être possible indépendamment du degré de liberté utilisé pour encoder chaque qubit de la paire. On peut donc envisager qu'un qubit de polarisation puisse être intriqué avec un qubit temporel.

Contributions

Nous présentons une étude expérimentale de la non-localité d'une source d'intrication temporelle caractérisée à l'aide d'*analyseurs temporels universels* (ATU) qui permettent, pour la première fois, de mesurer chaque qubit temporel dans une base arbitraire. La présence de l'intrication est révélée par la mesure de la visibilité de l'intrication. Cette mesure a été répétée plusieurs fois en utilisant différentes bases qui, lorsque représentées sur la sphère de Bloch, couvrent toutes les dimensions de cette dernière, mettant ainsi en évidence le caractère universel des ATU. Nous avons ensuite révélé la nature non-locale de notre source d'intrication temporelle avec un test de l'inégalité de Bell-CHSH. Grâce aux ATU, ce test a pu être répété plusieurs fois de sorte que, de test en test, le grand cercle de la sphère de Bloch contenant les bases de mesures utilisées pour un test donné était soumis à une rotation. L'ensemble des grands cercles utilisés couvre toutes les dimensions de la sphère de Bloch. Ceci nous a permis de vérifier directement que la valeur du paramètre S est invariante par rotation du grand cercle contenant les bases de mesure. Ces expériences ont d'abord été réalisées dans l'environnement contrôlé d'un laboratoire, puis répétées sur le terrain où un des photons de chaque paire est transmis sur une fibre optique souterraine de 12,4 km. Cette source peut aussi être interprétée comme une source d'*intrication hybride* où un qubit de polarisation est intriqué avec un qubit temporel. Elle pourrait s'avérer utile dans un réseau quantique composé de différents types de liens de transmission et nécessitant différents types d'encodages. Finalement, ces travaux ouvrent aussi la voie vers de nouveaux tests de la non-localité et à la réalisation de nouveaux protocoles de communication quantique à l'aide de l'intrication temporelle.

Publications associées

• F. Bussières, N. Godbout et W. Tittel, « Hybrid entanglement for optical quantum networks », *38th Annual Meeting of the Division of Atomic, Molecular, and Optical Physics,*

Calgary, Alberta, Canada, 2007 (présentation orale).

• F. Bussières, A. Rubenok, N. Godbout et W. Tittel, « Towards Photonic Hybrid Entanglement », *Frontiers in Optics 2007, San José, California*, 2007 (présentation orale).

• F. Bussières, J. A. Slater, J. Jin, N. Godbout, S. Hosier et W. Tittel, « Convertible quantum encodings and hybrid entanglement on a real-world fiber link ». *Quantum Communications and Quantum Imaging VII, San Diego, California*, août 2009 (présentation orale).

• F. Bussières, J. A. Slater, J. Jin, N. Godbout et W. Tittel, « Testing non-locality with universal time-bin qubit analyzers ». En préparation.

Pile ou face quantique (chapitre 5)

Problématique

Le pile ou face quantique est une primitive cryptographique où deux joueurs s'échangent à tour de rôle de l'information classique et quantique de façon à générer un bit aléatoire commun. L'utilisation de l'information quantique permet d'obtenir des protocoles tels qu'en présence d'un tricheur, ce dernier ne peut biaiser complètement le résultat. Malheureusement, la sécurité de tous les protocoles de pile ou face quantique antérieurs est sérieusement compromise en présence de pertes et de bruit dans le montage, rendant tous ces protocoles inutiles en pratique.

Contributions

Nous présentons le premier protocole de pile ou face quantique *tolérant aux pertes*. Nous montrons comment ce protocole peut être équilibré de sorte que la probabilité qu'un tricheur réussisse à obtenir le résultat désiré soit la même pour chaque joueur. Nous présentons également les stratégies de triche optimales. Nous discutons ensuite des conséquences du bruit dans un montage réaliste et nous présentons une nouvelle tâche, que nous nommons *pile ou face séquentiel*, basée sur l'application répétée de notre protocole de pile ou face quantique. Cette tâche est telle que sa sécurité n'est pas compromise en présence de pertes et de bruit. Finalement, à l'aide d'une source d'intrication temporelle, nous présentons la première démonstration expérimentale d'un protocole de pile ou face quantique tolérant aux pertes et nous discutons de son utilisation pour le pile ou face séquentiel. Ces expériences ont d'abord été réalisées dans l'environnement contrôlé d'un laboratoire, puis répétées sur le terrain où un des photons de chaque paire est transmis sur une fibre optique souterraine de 12,4 km.

Publications associées [10]

• G. Berlín, G. Brassard, F. Bussières et N. Godbout, « A new protocol for loss-tolerant quantum coin flipping », *Fourth Canadian Quantum Information Students' Conference, University*

10. L'ordre des auteurs de ces publications est alphabétique.

of Waterloo and Perimeter Institute, juin 2007 (présentation orale)

• G. Berlín, G. Brassard, F. Bussières et N. Godbout, « Loss-tolerant quantum coin flipping », *Proceedings of the Second International Conference on Quantum, Nano and Micro Technologies*, pp. 1–9, 2008.

• G. Berlín, G. Brassard, F. Bussières et N. Godbout, « A fair loss-tolerant quantum coin flipping protocol », *Proceedings of the Ninth International Conference on Quantum Communication, Measurement and Computing (QCMC)*, vol. 1110, pp. 384–387, American Institute of Physics, 2009.

• G. Berlín, G. Brassard, F. Bussières et N. Godbout, « Fair loss-tolerant quantum coin flipping », *Physical Review A (à paraître)*, 2009.

• G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater et W. Tittel, « Flipping quantum coins ». `arXiv:0904.3946`, 2009. Soumis pour publication.

• G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater et W. Tittel, « Loss-tolerant quantum coin flipping », *Biannual workshop of the Institut Transdisciplinaire d'Informatique Quantique, Magog, Québec*, mai 2009 (présentation orale).

• G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater et W. Tittel, « Flipping quantum coins ». *Conference on Quantum Information and Quantum Control, Toronto, Ontario*, août 2009 (présentation orale).

Chapitre 2

Manipulation de l'encodage temporel

Ce chapitre est divisé en deux parties. Tout d'abord, dans la section 2.1, nous proposons deux méthodes permettant d'implémenter une opération unitaire, arbitraire et déterministe sur un qubit temporel à l'aide de composants optiques tout-fibre. Nous montrons aussi comment utiliser ces méthodes pour mesurer un qubit temporel dans une base arbitraire. Une généralisation au cas d'un *qudit* temporel est ensuite présentée. Ce travail a pour but d'explorer les différentes façons de manipuler l'encodage temporel et d'élargir son champ d'application pour la communication quantique et pour le traitement de l'information quantique en général.

Ensuite, dans la section 2.2, nous proposons une implémentation tout-fibre du calcul quantique basé sur la mesure. Les méthodes développées dans la première partie de ce chapitre sont utilisées pour montrer comment créer un « cluster » optique arbitraire à l'aide de l'encodage temporel. Ensuite, nous montrons comment réaliser les *opérations en aval* essentielles à cette approche à l'aide de composants tout-fibre. Les propriétés de ces composants nous permettent d'envisager une réduction substantielle du temps nécessaire pour programmer ces opérations en aval par rapport aux autres méthodes réalisées jusqu'ici.

2.1 Opérations arbitraires et déterministes sur qubits temporels

Nous définissons d'abord les concepts de qubit encodé en polarisation et de qubit temporel.

2.1.1 Qubit encodé en polarisation

Un qubit encodé en polarisation peut être obtenu à l'aide d'un photon unique dans un état de polarisation donné. Les états de polarisation horizontale $|H\rangle$ et verticale $|V\rangle$ définissent une base orthonormée et leur combinaison linéaire permet d'obtenir tous les états à un qubit. Par exemple, l'état $|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ correspond à un photon de polarisation rectiligne à 45°. Ce type d'encodage est simple à manipuler à l'aide de composants optiques et propagation à l'air libre. Toutes les opérations unitaires sur un seul qubit peuvent être réalisées avec une

lame demi-onde placée entre deux lames quart d'onde, et une mesure dans une base arbitraire se fait à l'aide de ces mêmes composants et d'un cube polariseur [4]. [1]

La transmission de qubits en polarisation sur une longue distance a été réalisée à l'air libre avec l'aide de télescopes sur des distances de l'ordre de quelques kilomètres [86, 87] et même jusqu'à une centaine de kilomètres [88, 89]. La fibre optique est un autre moyen par lequel des qubits en polarisation peuvent être transmis. Cependant, tout lien de fibre optique standard installé dans un environnement non contrôlé est soumis à des fluctuations thermiques et à un stress mécanique entraînant une fluctuation aléatoire de la biréfringence de la fibre. La dérive de la polarisation doit alors être compensée, ce qui impose une difficulté technologique supplémentaire mais surmontable. La limite ultime est dictée par la largeur spectrale des photons. En effet, chaque tranche spectrale est soumise à une biréfringence différente des autres tranches, ce qui cause la décohérence du qubit en raison de la *dispersion modale de la polarisation de second-ordre.* [2] Malgré la présence biréfringence et la dispersion modale de la polarisation, plusieurs expériences récentes ont démontré que l'encodage en polarisation peut être transmis sur une distance pouvant atteindre 100 à 200 km dans la fibre unimodale standard [91, 92] ou dans une fibre à dispersion décalée [93].

2.1.2 Qubit temporel

L'encodage temporel de qubit [3] correspond à un photon en superposition de présence à l'intérieur de deux fenêtres temporelles mutuellement exclusives [94, 18]. Plus précisément, à l'aide de la fibre optique, un qubit temporel est généré lorsqu'un photon unique présent dans une impulsion de durée temporelle τ est incident sur le montage de la fig. 2.1. À la sortie du coupleur C, la fonction d'onde du photon est séparée en deux composantes et le photon se retrouve en superposition de parcourir le bras court et le bras long, le délai entre les bras étant $\Delta t \gg \tau$. À la sortie de l'interféromètre, les deux composantes désynchronisées sont combinées dans un coupleur 50/50. Le photon émerge alors par le bras inférieur du coupleur de sortie avec une probabilité de 50%. Lorsque c'est le cas, son état est donné par

$$|\psi\rangle = \cos\theta|t_0\rangle + \mathrm{e}^{i\varphi}\sin\theta|t_1\rangle, \tag{2.1}$$

où $t_1 - t_0 = \Delta t$. La définition formelle des états de base $|t_0\rangle$ et $|t_1\rangle$ est donnée ci-bas. Le paramètre θ est fixé par le taux de couplage du coupleur à l'entrée et φ correspond au déphasage entre les bras. Ce déphasage peut être sélectionné par le modulateur de phase MP. Cela per-

1. « Polarizing beamsplitter ».
2. Plus précisément, la dispersion modale de la polarisation de second ordre provient du fait que le délai de groupe (*differential group delay*) dépend de la longueur d'onde [90].
3. « Time-bin qubit ».

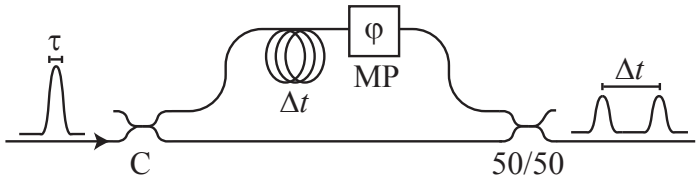

FIGURE 2.1 Circuit optique générant un qubit temporel. Les lignes représentent de la fibre optique, C est un coupleur (l'équivalent tout-fibre d'une lame séparatrice), MP est un modulateur de phase et 50/50 est le taux de couplage du coupleur de sortie.

met de générer tous les états à un qubit. On remarque finalement que le coupleur 50/50 peut être remplacé par un commutateur optique permettant de multiplexer temporellement les deux composantes dans la même fibre de sortie.

Les états de base $|t_0\rangle$ et $|t_1\rangle$ peuvent être formellement définis en exprimant le vecteur d'état du photon à l'aide la représentation de Fourier. Par exemple, l'état $|t_0\rangle$ peut être vu comme un photon unique contenu dans un paquet d'onde gaussien centré au temps t_0 :

$$|t_0\rangle \;=\; \int_{-\infty}^{\infty} \mathrm{d}\omega\, g(\omega-\omega_0)\, \mathrm{e}^{i\omega t_0}\, \hat{a}_\omega^\dagger\, |0\rangle \tag{2.2}$$

où, pour une distribution spectrale gaussienne, $g(\omega-\omega_0) = C\mathrm{e}^{-(\omega-\omega_0)^2/4\sigma^2}$, C est une constante, $\hat{a}_\omega^\dagger$ est l'opérateur de création d'un photon à la fréquence ω et $|0\rangle$ est l'état de Fock à 0 photon. Ainsi, on a

$$\begin{aligned}
\langle t_1|t_0\rangle &= \iint_{-\infty}^{\infty} \mathrm{d}\omega'\; \mathrm{d}\omega\, g(\omega'-\omega_0)\, g(\omega-\omega_0)\, \mathrm{e}^{-i\omega' t_1}\, \mathrm{e}^{i\omega t_0}\, \langle 0|\hat{a}_{\omega'}\hat{a}_\omega^\dagger|0\rangle && (2.3)\\
&= \iint_{-\infty}^{\infty} \mathrm{d}\omega'\; \mathrm{d}\omega\, g(\omega'-\omega_0)\, g(\omega-\omega_0)\, \mathrm{e}^{-i\omega' t_1}\, \mathrm{e}^{i\omega t_0}\, \delta(\omega-\omega') && (2.4)\\
&= \int_{-\infty}^{\infty} \mathrm{d}\omega\, g(\omega-\omega_0)^2\, \mathrm{e}^{-i\omega\Delta t} && (2.5)\\
&\sim \mathrm{e}^{-i\omega_0\Delta t}\mathrm{e}^{-2\sigma^2(\Delta t)^2}, && (2.6)
\end{aligned}$$

d'où on voit directement que si la séparation temporelle Δt est largement supérieure à la durée temporelle τ des états $|t_0\rangle$ et $|t_1\rangle$, alors $\langle t_1|t_0\rangle \sim \mathrm{e}^{-2\sigma^2(\Delta t)^2} \to 0$ car $\sigma \sim \tau^{-1}$. Les états $|t_0\rangle$ et $|t_1\rangle$ forment donc une base orthonormée. L'état d'un qubit temporel peut donc s'exprimer ainsi :

$$|\psi\rangle \;=\; \int_{-\infty}^{\infty} \mathrm{d}\omega\, g(\omega-\omega_0)\, \left(\cos\theta\, \mathrm{e}^{i\omega t_0} + \sin\theta\, \mathrm{e}^{i\omega(t_1+T)}\right) \hat{a}_\omega^\dagger\, |0\rangle \tag{2.7}$$

où nous avons redéfini t_1 comme $t_1 + T$, avec $T \ll \tau$, de sorte que ce petit déplacement correspond à un changement de phase beaucoup plus petit que la phase couverte par la durée de $|t_1\rangle$. Ainsi, on peut faire l'approximation que les paquets d'onde $|t_0\rangle$ et $|t_1\rangle$ sont quasi-monochromatiques et remplacer $\mathrm{e}^{i\omega T}$ par $\mathrm{e}^{i\omega_0 T}$ dans l'intégrale. On obtient l'expression suivante :

$$\begin{aligned} |\psi\rangle &= \cos\theta \int_{-\infty}^{\infty} \mathrm{d}\omega\, g(\omega-\omega_0)\, \mathrm{e}^{i\omega t_0}\, \hat{a}_\omega^\dagger\, |0\rangle \\ &+ \mathrm{e}^{i\omega_0 T} \sin\theta \int_{-\infty}^{\infty} \mathrm{d}\omega\, g(\omega-\omega_0)\, \mathrm{e}^{i\omega t_1}\, \hat{a}_\omega^\dagger\, |0\rangle, \end{aligned}$$

ce qui correspond formellement à l'éq. 2.1 en utilisant la définition 2.2.

Un qubit temporel est facilement mesuré dans la base $\mathcal{B}_+ = \{|t_0\rangle, |t_1\rangle\}$: il suffit d'observer le temps de détection. Il peut également être mesuré dans la base $\mathcal{B}_\times(\alpha) = \left\{\frac{1}{\sqrt{2}}(|t_0\rangle + \mathrm{e}^{i\alpha}|t_1\rangle), \frac{1}{\sqrt{2}}(|t_0\rangle - \mathrm{e}^{i\alpha}|t_1\rangle)\right\} \equiv \left\{|+\rangle_\alpha, |-\rangle_\alpha\right\}$ à l'aide de ce que nous nommons un *analyseur temporel standard* dont le circuit optique est présenté à la fig. 2.2. En réalité, cet analyseur temporel standard permet de mesurer à la fois dans la base $\mathcal{B}_+$ et dans la base $\mathcal{B}_\times(\alpha)$. Pour le comprendre, supposons d'abord que l'état incident est $|\pm\rangle_\alpha$ et considérons la branche de sortie du détecteur D_0. Une détection peut survenir à l'intérieur de trois fenêtre temporelles f_0, f_2 et f_1 séparées chronologiquement par Δt. Une détection dans f_0 (f_1) est causée par la composante $|t_0\rangle$ ($|t_1\rangle$) ayant parcourue le bras court (long) de l'interféromètre. Ainsi, une détection dans une de ces fenêtres correspond à une mesure dans la base $\mathcal{B}_+$. Une détection dans la fenêtre f_2 peut être causée soit par la composante $|t_0\rangle$ ayant parcourue le bras long, soit par la composante $|t_1\rangle$ ayant parcouru le bras court. Si les polarisations des deux composantes sont identiques, elles interfèrent et la probabilité qu'une détection survienne est proportionnelle au carré de la somme des amplitudes des deux possibilités, soit $|\mathrm{e}^{i\varphi} \pm \mathrm{e}^{i\alpha}|^2$, où φ est la phase appliquée sur $|t_0\rangle$ par le modulateur de phase MP. Le raisonnement est le même pour une détection dans la branche de D_1, sauf que la probabilité de détection dans f_2 est

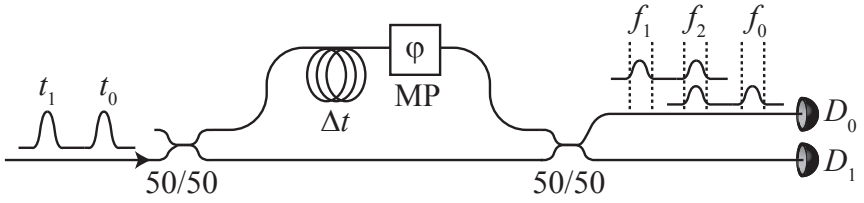

FIGURE 2.2 Circuit optique d'un *analyseur temporel standard* réalisant une mesure dans la base $\mathcal{B}_+$ avec une probabilité 1/2 ou dans la base $\mathcal{B}_\times(\varphi)$ avec une probabilité 1/2.

proportionnelle à $|e^{i\varphi} \mp e^{i\alpha}|^2$ en raison de l'unitarité des coupleurs. On voit immédiatement qu'en ajustant $\varphi = \alpha$, l'état $|+\rangle_\alpha$ ($|-\rangle_\alpha$) est détecté par D_0 (D_1) avec certitude, ce qui constitue une mesure dans la base $\mathcal{B}_\times(\alpha)$. Cet analyseur temporel standard permet donc de faire un choix aléatoire et passif de la base de mesure. Au total, la probabilité que la mesure se fasse dans la base $\mathcal{B}_+$ ($\mathcal{B}_\times(\alpha)$) est de 50%. Cependant, il ne permet pas de mesurer un qubit temporel dans une base arbitraire.

Un avantage de l'encodage temporel est que le montage de la fig. 2.2 fonctionne indépendamment de la polarisation du qubit : il suffit que la polarisation des composantes qui interfèrent soit la même. Il est cependant sensible à l'étalement temporel du paquet d'onde causé par la dispersion chromatique dans les fibres optiques. En effet, une transmission sur une longue distance cause éventuellement le chevauchement des composantes $|t_0\rangle$ et $|t_1\rangle$. Ce problème est surmonté soit en utilisant une fibre à dispersion nulle [95], soit en limitant sa largeur spectrale pour s'affranchir des effets de l'étalement ou encore en compensant la dispersion avec un milieu à dispersion de signe opposé à celle de la fibre utilisée [96]. Une deuxième difficulté rencontrée en manipulant cet encodage est que le déphasage φ entre les bras de l'interféromètre doit être stable. Cette difficulté peut être surmontée en choisissant un délai Δt suffisamment petit et en contrôlant bien la température de l'interféromètre de façon à s'affranchir de l'effet des fluctuations thermiques, ou encore en utilisant un laser à fréquence stabilisée pour sonder et ajuster la phase à la valeur désirée [95]. L'encodage temporel a été utilisé dans plusieurs expériences (la référence [9] présente une revue de son utilisation pour la distribution quantique de clés) et des qubits temporels ont été transmis sur une distance de l'ordre de 50 km dans une fibre à dispersion décalée [95, 97].

Comme tous les protocoles de communication quantique nécessitent des opérations à un qubit, une méthode générale permettant de réaliser des opérations arbitraires et déterministes sur un qubit temporel est souhaitable. On remarque du coup que cela permet aussi de réaliser une mesure dans une base arbitraire. Une telle méthode est un des ingrédients nécessaire à la réalisation d'une réalisation déterministe de plusieurs tâches comme la téléportation quantique [60], la permutation d'intrication [64] et le calcul quantique [4]. C'est dans le but de combler ce besoin que nous avons développé les deux premières méthodes générales permettant de réaliser des opérations arbitraires et déterministes sur un qubit temporel (section 2.1.4) ainsi qu'une généralisation au cas d'un qudit (section 2.1.5). Un des avantages qui ressort de cette étude, et qui est discuté à la section 2.2, est que la disponibilité commerciale de composants actifs tout-fibre nous permet d'espérer réaliser des opérations programmables à l'intérieur de quelques nanosecondes. En guise de comparaison, une opération sur un qubit en polarisation se propageant à l'air libre nécessite actuellement un temps de programmation d'environ 150 ns [81].

2.1.3 Autres types d'encodage

Outre l'encodage temporel et en polarisation, il existe des encodages exploitant les autres degrés de liberté de la lumière, soit le mode spatial [98], la fréquence [99, 100, 101] et le moment orbital angulaire [102]. Nous invitons le lecteur à consulter ces références pour plus d'information.

2.1.4 Opérations déterministes sur un qubit temporel

Pour réaliser une opération arbitraire sur un qubit temporel, les composantes $|t_0\rangle$ et $|t_1\rangle$ doivent, en général, interférer. Ceci requiert l'utilisation d'interféromètres et de commutateurs optiques. Nous commençons par décrire deux méthodes permettant d'atteindre ce but, la première ayant recours à l'encodage en polarisation, la deuxième à l'encodage spatial. Ces deux méthodes peuvent être réalisées à l'aide de technologies disponibles commercialement. Dans cette section, la fibre est supposée unimodale. Tous les composants optiques discutés ici sont disponibles commercialement aux longueurs d'onde de la télécommunication, soit aux alentours de 1550 nm. Cependant, les méthodes présentées ne se limitent pas à cette longueur d'onde, ni à la transmission par fibre optique. Elles peuvent être transposées directement à n'importe quel type de guidage optique ou encore à une transmission à l'air libre.

Opération déterministe à l'aide de l'encodage en polarisation

La première méthode proposée tire profit du fait que les opérations sur un qubit en polarisation peuvent être réalisées à l'aide d'un contrôleur de polarisation tout-fibre [103]. Pour cela, le qubit temporel est converti en un qubit en polarisation pour effectuer l'opération, et est ensuite converti à nouveau vers un qubit temporel. Le circuit optique nécessaire est montré à la fig. 2.3. Premièrement, un qubit temporel polarisé horizontalement est incident sur un commutateur optique 1×2 guidant respectivement les composantes $|t_0\rangle$ et $|t_1\rangle$ vers les bras inférieur et supérieur. Dans le bras inférieur, la polarisation de la composante $|t_0\rangle$ est

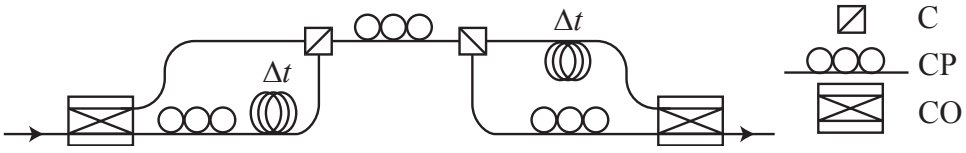

FIGURE 2.3 Circuit optique implémentant une opération arbitraire et déterministe sur un qubit temporel à l'aide de l'encodage en polarisation. C est un cube polariseur, CP est un contrôleur de polarisation et CO est un commutateur optique.

tournée à la verticale et un délai Δt la synchronise avec la composante $|t_1\rangle$. Le cube polariseur transmet $|t_1\rangle$ et réfléchit $|t_0\rangle$ de sorte qu'à sa sortie, le qubit temporel est converti en un qubit en polarisation selon la correspondance $|t_0\rangle \rightarrow |V\rangle$ et $|t_1\rangle \rightarrow |H\rangle$. Le contrôleur de polarisation tout-fibre permet ensuite de réaliser l'opération désirée avec une perte négligeable. Le reste du circuit agit à l'inverse de la première section et convertit à nouveau le qubit en polarisation en qubit temporel. Ce montage permet donc de réaliser toutes les opérations sur un qubit temporel. Notons que ce circuit requiert que la polarisation du qubit incident soit horizontale.

Pour une opération donnée, les commutateurs sont les seuls composants actifs et la fréquence de commutation est cruciale. En effet, plus cette dernière est élevée, plus le délai Δt entre les composantes peut être petit et plus les interféromètres sont faciles à stabiliser en température. Pour établir un critère de tolérance, définissons $f = 1/\Delta t$, la fréquence de commutation, ainsi que $\Delta L = c\Delta t/n_g = c/n_g f$, la différence de marche entre les bras, où n_g est l'indice de groupe dans la fibre. La différence de phase accumulée entre les deux bras de l'interféromètre est

$$\begin{aligned} \Delta\phi &= \phi_1 - \phi_2 && (2.8)\\ &= k n_e L_1 - k n_e L_2 && (2.9)\\ &= k n_e \Delta L, && (2.10) \end{aligned}$$

où k est le nombre d'onde dans le vide et n_e est l'indice effectif dans la fibre. Lorsque la température change, la différence varie comme

$$\frac{\mathrm{d}\Delta\phi}{\mathrm{d}T} = k\left(\frac{\mathrm{d}n_e}{\mathrm{d}T}\Delta L + n_e\frac{\mathrm{d}\Delta L}{\mathrm{d}T}\right). \qquad (2.11)$$

Considérant que l'indice varie linéairement avec la température, $\mathrm{d}n_e/\,\mathrm{d}T = \beta$, et que la dilatation suit la loi habituelle $\mathrm{d}L_i/\,\mathrm{d}T = \alpha L_i$ $(i = 1, 2)$, on trouve

$$\begin{aligned} \frac{\mathrm{d}\Delta\phi}{\mathrm{d}T} &= k\Delta L\,(\beta + n_e\alpha) && (2.12)\\ &= \frac{kc}{n_g f}\,(\beta + n_e\alpha) && (2.13) \end{aligned}$$

Pour la fibre standard, les valeurs usuelles sont $\beta = 10^{-5}$ K^{-1}, $\alpha = 5 \times 10^{-7}$ K^{-1} et $n_e \approx n_g \approx 1{,}45$, ce qui donne $\mathrm{d}\Delta\phi/\,\mathrm{d}T \approx (9 \times 10^9)/f$ rad/K. En fixant le critère de stabilité à $\mathrm{d}\Delta\phi \leq \pi/20$ et $\mathrm{d}T = 0{,}1$ K, on a $f \geq 5{,}7$ GHz, soit un délai $\Delta T \leq 0{,}18$ ns. On peut donc établir que la stabilisation thermique requiert une stabilité de l'ordre du dixième de degré K pour une fréquence de 10 GHz, au centième de degré K pour un fréquence de 1 GHz

et ainsi de suite. Une stabilité au dixième de degré K peut être obtenue avec un système de stabilisation de la température. À des fréquences inférieures, un système de verrouillage de la phase serait nécessaire pour utiliser le système indéfiniment.

Il est aussi nécessaire de considérer les pertes d'insertion des composants. Les pertes les plus importantes proviennent du cube polariseur, de l'ordre de 0,4 dB par unité, et des commutateurs électrooptiques, de l'ordre de 2 à 3 dB par unité. Cela donne une perte totale estimée de 4,8 dB, soit une transmission d'environ 33%. En principe, rien ne limite la réduction des pertes d'insertion de ces composants et il est raisonnable d'espérer une amélioration de la transmission de la méthode proposée avec l'amélioration de la technologie.

Le montage de la fig. 2.3 permet également de mesurer un qubit temporel dans une base arbitraire. Pour ce faire, il suffit de mesurer le qubit juste après le deuxième cube polariseur, tel que montré sur la fig. 2.4. La combinaison du contrôleur de polarisation et du cube polariseur permet de sélectionner la base dans laquelle on désire mesurer le qubit en question. Ce circuit agit comme un *analyseur temporel universel* (ATU). On note que le commutateur optique peut être remplacé par un coupleur 50/50. Le circuit permet alors de réaliser une mesure dans une base arbitraire avec une probabilité de 50%, et dans la base B_+ le reste du temps.

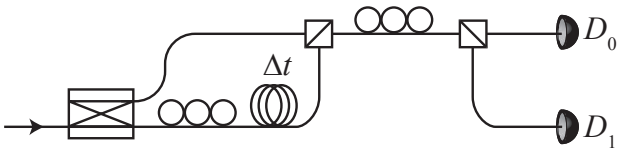

FIGURE 2.4 Analyseur temporel universel : circuit optique implémentant une mesure dans une base arbitraire sur un qubit temporel à l'aide de l'encodage en polarisation.

Opération déterministe à l'aide de l'encodage spatial

La deuxième méthode proposée pour réaliser une opération déterministe fonctionne à l'aide de l'encodage spatial. Un qubit spatial correspond à une impulsion à un photon en superposition de parcourir deux fibres optiques distinctes [98] et peut être généré à l'aide d'un coupleur. Par exemple, l'état du photon juste après le premier coupleur du montage de la fig. 2.1 correspond à un qubit spatial. Le circuit permettant de réaliser une opération arbitraire et déterministe sur le qubit temporel est présenté à la fig. 2.5 et fonctionne comme suit. Un qubit temporel est incident par la gauche sur un commutateur optique 1×2 qui guide respectivement les composantes $|t_0\rangle$ et $|t_1\rangle$ vers les bras supérieur et inférieur. Ensuite, un délai Δt sur le bras supérieur permet de synchroniser les deux composantes et, par conséquent,

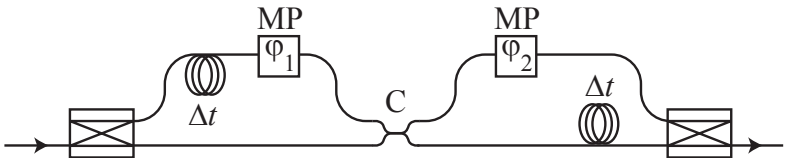

FIGURE 2.5 Circuit optique réalisant une opération sur un qubit temporel à l'aide de l'encodage spatial.

le qubit temporel est converti en qubit spatial. Par la suite, les deux composantes du qubit spatial interfèrent au coupleur. En choisissant le taux de couplage de ce dernier ainsi que les déphasages φ_1 et φ_2 introduits par les modulateurs de phase, on peut réaliser toutes les opérations unitaires possibles sur le qubit spatial [98]. Lorsque cela est fait, le reste du circuit convertit à nouveau vers l'encodage temporel. Ce circuit permet donc d'effectuer toutes les opérations unitaires possibles sur un qubit temporel.

Pour réaliser une opération donnée, les commutateurs sont les seuls composants actifs et les considérations de stabilité thermique sont les mêmes que pour le circuit de la fig. 2.3. À l'aide de la technologie tout-fibre, tous les composants sauf les commutateurs peuvent être fabriqués avec une très faible perte. Par exemple, la perte d'un coupleur tout-fibre est de l'ordre de 0,1 dB ou moins. La perte totale estimée se situe entre 4 et 5 dB. L'avantage de cette méthode réside dans le fait que, en principe, il est insensible à la polarisation du qubit temporel incident.

2.1.5 Opérations déterministes sur qudits temporels

Le concept du qubit se généralise facilement au cas où l'observable possède $d > 2$ états propres. On parle alors de qudit. Plusieurs travaux théoriques ont montré qu'il est parfois avantageux d'utiliser des qudits et nous en citons ici quelques exemples. Pour la distribution quantique de clés, les qudits possèdent une meilleure tolérance au bruit [104] et ils permettent d'améliorer la capacité d'un canal quantique [105]. L'utilisation de qutrits ($d = 3$) permet de simplifier certaines tâches en complexité de la communication [106] et ils fournissent une solution au problème de l'accord byzantin [107]. Les qudits intriqués permettent aussi, en principe, d'observer une séparation plus importante entre les théories à variables locales cachées et la mécanique quantique [37, 38, 108] et d'augmenter la tolérance au bruit de certaines inégalités de Bell [109].

Tout d'abord, montrons comment générer un qudit temporel. Pour ce faire, il suffit de généraliser le circuit de la fig. 2.1 au cas où l'impulsion incidente à un photon est séparée en d composantes au lieu de 2 à l'aide d'un coupleur $1 \times d$, tel qu'illustré à la fig. 2.6. Notons

qu'un coupleur $1 \times d$ peut être fabriqué à l'aide de $d-1$ coupleurs 2×2 et qu'un commutateur $d \times 1$ requiert $d-1$ commutateurs 2×2. Le nombre de composants nécessaires croît donc linéairement avec la dimension.

Pour réaliser une opération sur un qudit temporel, on procède en trois étapes. La première consiste à convertir le qudit temporel en un qudit spatial, la deuxième à réaliser l'opération unitaire sur le qudit spatial et la troisième à reconvertir vers l'encodage temporel à nouveau. Commençons par montrer comment convertir un qudit temporel en un qudit spatial. Pour ce faire, il suffit d'inverser le processus de génération. Tout d'abord, le qudit temporel est incident sur un commutateur $1 \times d$ tel qu'illustré à la fig. 2.7. Ce dernier démultiplexe les d composantes temporelles en d composantes spatiales et les synchronise toutes à l'aide des délais appropriés. En deuxième lieu, il faut appliquer l'opération désirée sur le qudit spatial obtenu. Pour cela, on utilise un résultat de M. Reck, A. Zeilinger, H. J. Bernstein et P. Bertani [110] montrant comment réaliser n'importe quelle opération sur un qudit spatial à l'aide de $(d-1)d/2$ coupleurs 2×2 ou moins ainsi que de d modulateurs de phase (ce résultat est détaillé au paragraphe suivant). En dernier lieu, on re-convertit le qubit spatial en qubit temporel à l'aide d'un circuit similaire à celui de la fig. 2.7 mais utilisé en sens inverse. Le nombre de composants optiques nécessaires croît selon $\mathcal{O}(d^2)$, où d est la dimension du qudit.

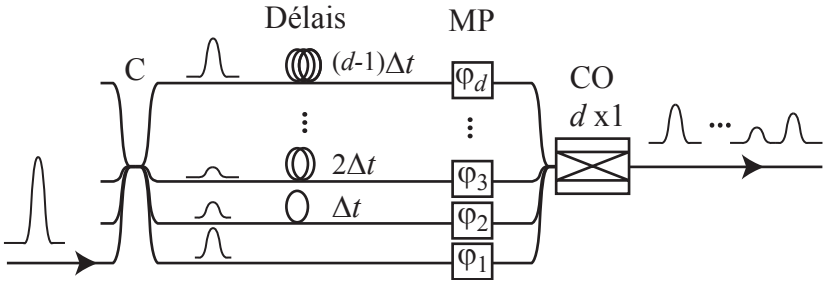

FIGURE 2.6 Circuit optique générant un qudit temporel.

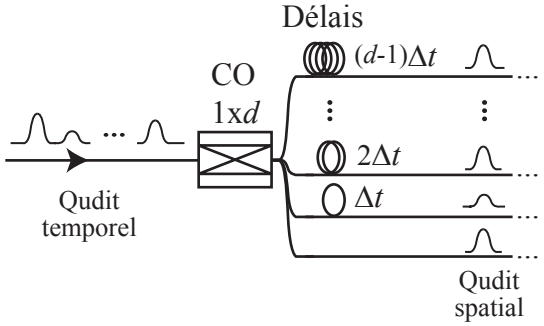

FIGURE 2.7 Circuit optique permettant de convertir un qudit temporel en un qudit spatial.

En pratique, cette méthode serait très difficile à réaliser pour $d \geq 3$ et pour une séparation de l'ordre de 1 ns ou plus entre les composantes temporelles. En effet, la stabilisation de la phase des chemins optiques serait alors très difficile à obtenir. Néanmoins, il est envisageable qu'une réduction substantielle de la séparation entre les composantes élimine cette contrainte et rende la méthode proposée réalisable expérimentalement.

2.1.6 Application à la distribution quantique de clés avec qutrits

Nous détaillons ici le résultat de Reck *et al.* [110] dans le but de l'appliquer à un exemple précis nécessitant la manipulation de qutrits temporels. Considérons un photon unique en superposition de présence dans d modes spatiaux (c'est-à-dire d fibres optiques) indexés de 1 à d. Nous notons $B_{m,n}$ la matrice de transfert d'un coupleur 2×2 couplant les modes m et n, ainsi que $B'_{m,n}$ l'extension mathématique de $B_{m,n}$ à une matrice $d \times d$ agissant uniquement sur le sous-espace des modes m et n. Spécifiquement, $B'_{m,n}$ est la matrice identité I de dimension $d \times d$ dont les éléments I_{mm}, I_{mn}, I_{nm} et I_{nn} sont remplacés par les éléments de $B_{m,n}$. La référence [110] montre comment toute matrice unitaire de dimension d, que nous notons $\mathrm{U}(d)$, est factorisable en une séquence de matrices $B'_{m,n}$. Cette factorisation s'écrit ainsi :

$$\mathrm{U}(d) = P \cdot \tilde{B}'_{2,1} \ldots \tilde{B}'_{d-1,1} \cdot \tilde{B}'_{d,1} \,, \tag{2.14}$$

où $\tilde{B}'_{d,1}$ est une séquence de $d-1$ matrices 2×2 couplant les modes d et $d-1$, d et $d-2$, et ainsi de suite jusqu'à d et 1 :

$$\tilde{B}'_{d,1} = B'_{d,1} \ldots B'_{d,d-2} \cdot B'_{d,d-1} \,. \tag{2.15}$$

La décomposition des matrices $\tilde{B}'_{d-1,1}, \ldots, \tilde{B}'_{2,1}$ est similaire. La matrice P correspond à une correction de phase appliquée sur chaque mode et est donc diagonale. Ainsi, la décomposition de $\mathrm{U}(d)$ nécessite $(d-1)d/2 \sim \mathcal{O}(d^2)$ coupleurs 2×2. Comme un qudit temporel peut être converti en qudit spatial et vice-versa, la décomposition ci-haut montre comment réaliser n'importe quelle transformation unitaire $\mathrm{U}(d)$ sur un qudit temporel.

Voici un exemple de cette décomposition. Nous l'appliquons au cas du protocole de distribution quantique de clés proposé dans la référence [111]. Ce protocole, basé sur l'utilisation de qudits, est intéressant car il permet en principe plus de résistance au bruit expérimental que le protocole BB84 utilisant des qubits [104]. Pour générer une clé, Alice choisit au hasard un état qutrit parmi un ensemble de douze états puisé parmi quatre bases mutuellement non biaisées [4] et l'envoie à Bob. Notons $\{|a\rangle, |b\rangle, |c\rangle\}$ la première de ces quatre bases. La deuxième

4. « Mutually unbiased ».

base peut être choisie comme suit :

$$|a'\rangle = (|a\rangle + |b\rangle + |c\rangle)/\sqrt{3}\,, \tag{2.16}$$
$$|b'\rangle = (|a\rangle + \mathrm{e}^{2\pi i/3}|b\rangle + \mathrm{e}^{-2\pi i/3}|c\rangle)/\sqrt{3}\,, \tag{2.17}$$
$$|c'\rangle = (|a\rangle + \mathrm{e}^{-2\pi i/3}|b\rangle + \mathrm{e}^{2\pi i/3}|c\rangle)/\sqrt{3}\,. \tag{2.18}$$

Les troisième et quatrième bases sont données par une permutation cyclique des états suivants :

$$(\mathrm{e}^{2\pi i/3}|a\rangle + |b\rangle + |c\rangle)/\sqrt{3}\,, \tag{2.19}$$
$$(\mathrm{e}^{-2\pi i/3}|a\rangle + |b\rangle + |c\rangle)/\sqrt{3}\,. \tag{2.20}$$

Suivant la réception du qutrit, Bob le mesure dans une des quatre bases choisie aléatoirement. Si les bases de préparation et de mesure sont identiques, Alice et Bob conservent le résultat. Avec des qutrit temporels, Bob peut choisir la première base comme étant celle du temps d'arrivée des photons. Pour la deuxième base, Bob a besoin d'appliquer une transformation unitaire U de dimension 3. Cette transformation est donnée par

$$U = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \mathrm{e}^{-2\pi i/3} & \mathrm{e}^{2\pi i/3} \\ 1 & \mathrm{e}^{2\pi i/3} & \mathrm{e}^{-2\pi i/3} \end{pmatrix}. \tag{2.21}$$

En se basant sur l'éq. 2.14, U se factorise comme suit :

$$U = P \cdot B'_{2,1} \cdot B'_{3,1} \cdot B'_{3,2}\,, \tag{2.22}$$

où les matrices 2×2 $B_{3,2}$, $B_{3,1}$ et $B_{2,1}$ associées à $B'_{3,2}$, $B'_{3,1}$ et $B'_{2,1}$ sont données par :

$$B_{3,2} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathrm{e}^{i\pi/3} & 1 \\ \mathrm{e}^{4\pi i/3} & 1 \end{pmatrix}, \tag{2.23}$$
$$B_{3,1} = \frac{1}{\sqrt{3}} \begin{pmatrix} \sqrt{2}\,\mathrm{e}^{-i\pi/3} & 1 \\ \mathrm{e}^{-i\pi/3} & -\sqrt{2} \end{pmatrix}, \tag{2.24}$$
$$B_{2,1} = \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ -i & 1 \end{pmatrix}. \tag{2.25}$$

On remarque tout d'abord que les matrices $B_{3,2}$ et $B_{2,1}$ correspondent à des coupleurs 50/50 à une phase près. La matrice $B_{3,1}$ correspond à un coupleur 33,3/66,6 à une phase relative

près. Ces coupleurs peuvent être fabriqués à l'aide de la technologie tout-fibre.

Le circuit optique réalisant U est montré à la fig. 2.8. Premièrement, un commutateur optique 1×3 combiné avec les délais Δt et $2\Delta t$ convertit le qutrit temporel en qutrit spatial. Deuxièmement, la transformation U est appliquée à l'aide de trois coupleurs 2×2. La dernière section du circuit re-convertit vers l'encodage temporel. Pour mesurer dans les troisième et quatrième bases, on peut montrer qu'on peut utiliser le même circuit sur lequel on aura ajouté des modulateurs de phase sur chaque mode entre les coupleurs.

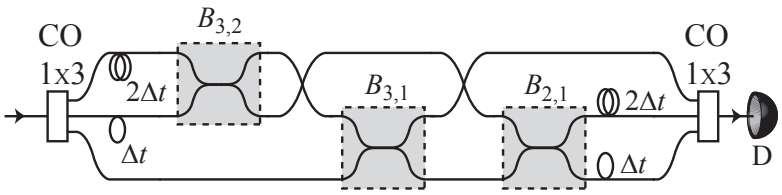

FIGURE 2.8 Circuit optique permettant de mesurer de façon déterministe les qutrits temporels du protocole de distribution quantique de clés de la référence [111].

2.2 Calcul quantique tout-fibre

Cette section traite de l'application des méthodes développées à la section 2.1 au *calcul quantique basé sur la mesure* (CQBM). Spécifiquement, nous montrons comment il est en principe possible de réaliser des circuits optiques tout-fibre réalisant les éléments essentiels du CQBM utilisant l'encodage temporel. Notre but n'est pas de couvrir tous les détails de ce modèle de calcul mais bien de discuter de son implémentation.

2.2.1 Calcul quantique basé sur la mesure avec optique linéaire

Une des difficultés majeures inhérente à l'implémentation d'un ordinateur quantique basé sur l'optique est la faiblesse de l'interaction non-linéaire entre photons. Ceci rend les portes quantiques à deux qubits photoniques très difficiles à réaliser. Pour surmonter ce problème, E. Knill, R. Laflamme et G. Milburn (KLM) ont développé une façon de créer des portes quantiques à plusieurs qubits n'utilisant que des éléments optiques linéaires mais avec le compromis de réduire probabilité de réussite du calcul à moins de 100% [77]. Cette approche est conceptuellement importante mais reste très difficile à implémenter car elle requiert une stabilité interférométrique entre un très grand nombre de modes optiques et a un coût technologique prohibitif. Le modèle du CQBM propose une approche différente en déplaçant la complexité vers la génération d'un état à plusieurs qubits intriqués mutuellement et en

réduisant la complexité du traitement à celui de la mesure projective de qubits individuels dans certaines bases [78]. Dans ce modèle, un *cluster*[5] de qubits intriqués peut être représenté par un graphe bidimensionnel (fig. 2.9) où chaque sommet représente un qubit préparé dans l'état $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, et où chaque arête indique que la porte à 2 qubits CZ a été appliquée. Cette porte peut être représentée par l'équation $CZ|ij\rangle = (-1)^{ij}|ij\rangle$, où $i, j \in \{0, 1\}$.

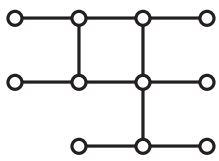

FIGURE 2.9 *Cluster* arbitraire : chaque sommet correspond à un qubit préparé dans l'état $|+\rangle$ et chaque arête indique que la porte CZ a été appliquée.

Suivant la création d'un cluster, le traitement débute et consiste en l'application séquentielle de mesures à un qubit dans certaines bases spécifiques. L'algorithme à implémenter indique le sous-ensemble de qubits qui seront mesurés. Spécifiquement, un premier sous-ensemble de qubits est mesuré, chacun dans une base pré-définie. Les résultats des mesures définissent les bases de mesures à utiliser sur les qubits d'un deuxième sous-ensemble (distinct du premier). Ces *opérations en aval*[6] sont répétées jusqu'à ce que l'algorithme se termine. L'état des qubits restants contient le résultat du calcul, mais son extraction nécessite d'abord l'application de corrections à un qubit avant de les mesurer individuellement. Ce modèle de calcul repose sur le fait que l'information est téléportée d'un ensemble de qubits à un autre [79] et le traitement repose sur le choix des bases de mesures. En pratique, la difficulté reliée à l'implémentation de ce modèle repose essentiellement sur la génération du cluster initial.

Une des approches qui a été proposée pour générer un état cluster est d'utiliser des portes probabilistes à 2 qubits de type *fusion* [85]. Cette approche est réaliste car le coût technologique associé à son implémentation est beaucoup moins important que celui de KLM [77]. Ces portes, construites uniquement à partir de composants optiques linéaires, permettent de fusionner deux clusters en un seul de taille plus grande. La fig. 2.10 illustre deux variétés de la porte *fusion* appliquées sur deux clusters encodés en polarisation. La probabilité de réussite de chacune est, dans le case idéal, égale à 50%. Le processus est répété jusqu'à l'obtention du cluster désiré. Les clusters à deux qubits initiaux peuvent être créés par conversion paramétrique spontanée (cf. sections 3.1 et 4.1.2).

5. Une traduction possible du mot anglais « cluster » est *grappe*. Cependant, nous prenons la liberté d'utiliser directement le terme *cluster*.

6. « Feedforward operations ».

La possibilité d'implémenter un circuit simple de CQBM utilisant la porte *fusion* de type I a été démontrée par deux groupes [80, 112] à l'aide de l'encodage en polarisation. Comme nous l'avons mentionné à la section 2.1.1, le traitement de cet encodage à l'air libre peut, *a priori*, sembler simple. Cependant, l'implémentation des opérations en aval, un des éléments essentiel de ce modèle de calcul, est plus ardu. Par exemple, supposons qu'un délai de 10 ns est réservé pour réaliser la mesure, le traitement classique et le transfert des commandes à un appareil optique actif utilisé pour appliquer l'opération en aval sur un qubit du cluster. Durant chaque cycle, les autres qubits doivent être stockés dans une ligne à délai optique d'au moins 3 m. La propagation de faisceaux gaussiens sur une distance de 10 m ou plus créera alors deux difficultés importantes qui affecteront inévitablement le chevauchement des faisceaux nécessaire à la réalisation des interféromètres. Premièrement, un faisceau possédant un « waist » de 1 mm aura diffracté au-delà de sa longueur de Rayleigh, qui est de l'ordre de

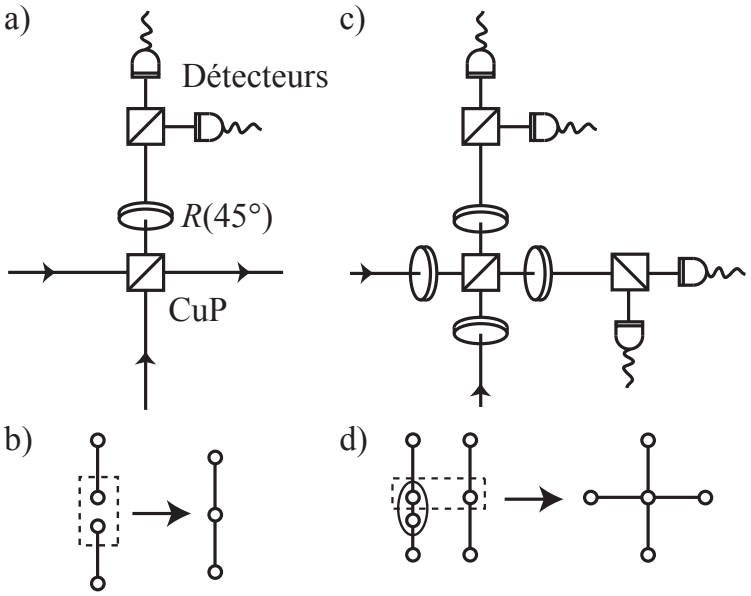

FIGURE 2.10 Représentation des portes *fusion* avec clusters encodés en polarisation. CuP est un cube polariseur et la porte à 1 qubit $R(45°)$ correspond à une lame demi-onde tournant la polarisation de 45°. Un qubit de chaque cluster (compris dans la boîte pointillée) est incident sur la porte *fusion*. a) porte *fusion* de type I : la fusion réussit si un seul photon est détecté, ce qui survient avec une probabilité de 50% dans le cas idéal (ceci nécessite un détecteur capable de discerner le nombre de photons). L'échec résulte en la disparition des arêtes connectant les deux qubits de chaque cluster. b) Lorsque l'opération réussit, les deux clusters sont fusionnés. c) porte *fusion* de type II : la fusion réussit si chaque détecteur détecte un photon, ce qui survient avec un probabilité de 50% dans le cas idéal. L'échec produit un cluster avec un encodage redondant et laisse l'intrication initiale des clusters intacte. d) Les deux qubits compris dans l'ovale sont encodés de façon redondante. Le cluster produit en cas de réussite est illustré.

2 m. Deuxièmement, une perturbation minime de la direction du vecteur d'onde du faisceau aura une très grande répercussion sur la position de celle-ci après une dizaine de mètres ou plus. Ces deux difficultés peuvent être éliminées avec l'utilisation de la fibre optique comme milieu de guidage sur des distances arbitraires. Pour cette raison, la fibre optique est un candidat très intéressant pour la mise en œuvre d'un circuit optique de calcul quantique.

Dans cette section, nous étudions la possibilité de réaliser les éléments de base du CQBM dans une architecture tout-fibre. Dans cette implémentation, chaque sommet du graphe de la fig. 2.9 est un photon unique transmis dans une fibre optique et est utilisé pour coder un qubit temporel. Un cluster de deux qubits correspond alors à deux qubits temporels intriqués. La génération d'un tel état est discuté à la section 4.1.2. Il suffit pour l'instant de supposer que nous avons la possibilité de créer deux qubits dans l'état intriqué suivant : $\frac{1}{\sqrt{2}}(|t_0, t_0\rangle + |t_1, t_1\rangle)$. Un cluster à deux qubits est généré en appliquant la porte Hadamard à un qubit sur chacun d'eux. L'état est alors $\frac{1}{2}(|t_0, t_0\rangle + |t_0, t_1\rangle + |t_1, t_0\rangle - |t_1, t_1\rangle)$.

La suite de la section 2.2 est divisée ainsi. Premièrement, la section 2.2.2 présente deux circuits optiques tout-fibre permettant de réaliser les éléments essentiels du CQBM. Deuxièmement, la section 2.2.3 présente une discussion portant sur quelques aspects techniques inhérents à cette proposition.

2.2.2 Génération de clusters et traitement

Génération d'un cluster temporel à l'aide de l'encodage spatial

Nous expliquons d'abord comment transcrire la porte *fusion* de type I (fig. 2.10-a) vers l'encodage temporel. Premièrement, l'équivalent temporel du cube polariseur CuP est un commutateur optique 2×2. Ce type de commutateur est possible à réaliser à l'aide de la technologie électrooptique utilisée en télécommunication et est disponible commercialement. Des fréquences de commutation aussi élevées que 10 GHz sont possibles. Ce commutateur imite le CuP en laissant la composante $|t_0\rangle$ poursuivre son chemin tandis que la composante $|t_1\rangle$ est commutée vers l'autre branche de sortie du commutateur.

La rotation $R(45°)$ est définie par

$$R(45°)|t_0\rangle = \frac{1}{\sqrt{2}}(|t_0\rangle + |t_1\rangle) \quad \text{et} \quad R(45°)|t_1\rangle = \frac{1}{\sqrt{2}}(-|t_0\rangle + |t_1\rangle). \tag{2.26}$$

Cette transformation peut être réalisée à l'aide du circuit optique basé sur une conversion à l'encodage spatial de la fig. 2.5. Pour ceci, le taux de couplage du coupleur central requis est

de 50/50 et nous supposerons que sa matrice de transfert est donnée par

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}. \tag{2.27}$$

En prenant les phases φ_1 et φ_2 égales à π, l'opération $R(45°)$ est obtenue. De la même façon, l'opération Hadamard, définie comme

$$\hat{H}|t_0\rangle = \frac{1}{\sqrt{2}}(|t_0\rangle + |t_1\rangle) \quad \text{et} \quad \hat{H}|t_1\rangle = \frac{1}{\sqrt{2}}(|t_0\rangle - |t_1\rangle), \tag{2.28}$$

est obtenue en prenant $\varphi_1 = 0$ et $\varphi_2 = \pi$. Tel qu'expliqué ci-haut, celle-ci est nécessaire pour créer les clusters à deux qubits.

La fig. 2.11 montre la porte *fusion* de type I résultante. On note que contrairement à la fig. 2.5, le deuxième commutateur optique n'est pas nécessaire et on peut mesurer directement à la sortie du coupleur. On rappelle que cette porte réussit lorsqu'un et un seul photon est détecté. La probabilité de réussite est, dans le cas idéal, de 50%.

Le circuit général de la fig. 2.5 peut également être utilisé pour implémenter la porte *fusion* de type II tel que présenté à la fig. 2.12. Quatre portes $R(45°)$ sont alors nécessaires et un commutateur optique joue le rôle du cube polariseur. On rappelle que la probabilité de réussite de cette porte est égale à 50% dans le cas idéal mais ne requiert pas l'utilisation d'un détecteur capable de discerner le nombre de photons détectés.

Traitement à l'aide de l'encodage spatial

Tel que mentionné dans l'introduction de cette section, le traitement de clusters nécessite deux ingrédients : la possibilité de mesurer chaque qubit individuellement dans une base spécifique et la possibilité d'appliquer certaines corrections (opérations à un qubit) à l'ensemble des qubits contenant le résultat du calcul. Ces mesures et corrections doivent se faire

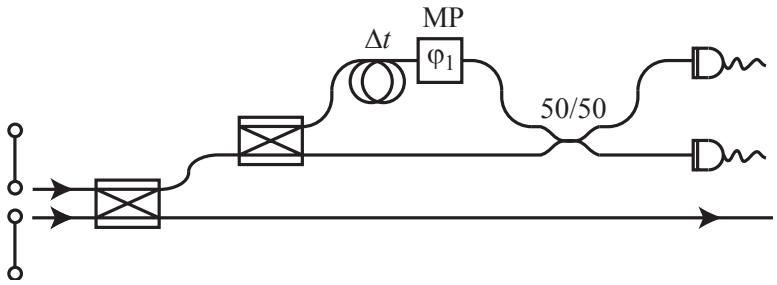

FIGURE 2.11 Porte *fusion* de type I basé sur la conversion d'un qubit temporel en qubit spatial. On prend $\varphi_1 = \pi$.

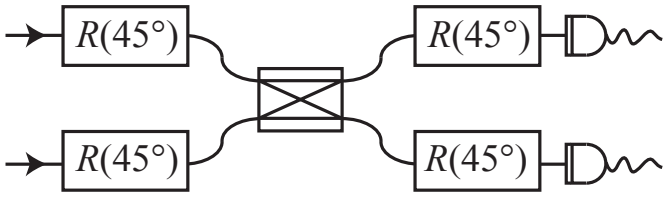

FIGURE 2.12 Porte *fusion* de type II basée sur la conversion d'un qubit temporel en qubit spatial. La transformation $R(45°)$ est réalisée à l'aide du circuit de la fig. 2.5.

en aval, c'est-à-dire que les bases de mesures et les corrections à effectuer dépendent du résultat des mesures précédentes.

On peut montrer [79] que les bases de mesures nécessaires sont obtenues en appliquant la transformation $R_z(\pm\theta)$, représentée par

$$\begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}, \tag{2.29}$$

suivie de la porte Hadamard et d'une mesure dans la base de calcul. Dans l'encodage temporel, la porte $R_z(\pm\theta)$ est obtenue avec un modulateur de phase appliquant une phase $-\theta/2$ sur la composante $|t_0\rangle$ et $\theta/2$ sur $|t_1\rangle$. En résumé, chaque mesure à un qubit peut être réalisée avec le circuit optique de la fig. 2.13.

L'algorithme réalisé détermine à l'avance la valeur des phases θ requises. Par contre, le signe de l'argument de $R_z(\pm\theta)$ est déterminé par le résultat des mesures précédentes. Par conséquent, il faut d'abord calculer (classiquement) le signe de l'argument et le fournir en aval au modulateur de phase. Pendant ce temps, les autres qubits peuvent être stockés à l'aide de lignes à délai.

Lorsque le traitement est terminé, des corrections peuvent être nécessaires. Un calcul ne requiert que deux corrections possibles. La première correspond à la matrice de Pauli σ_x, définie par $|t_0\rangle \rightarrow |t_1\rangle$ et $|t_1\rangle \rightarrow |t_0\rangle$. Comme cette correction est suivie d'une mesure dans la base de calcul, elle peut s'appliquer en inversant la convention temporelle. Autrement dit, une détection au temps t_0 correspond au résultat t_1 et vice versa. La deuxième est la matrice de Pauli σ_z, définie par $|t_0\rangle \rightarrow |t_0\rangle$ et $|t_1\rangle \rightarrow -|t_1\rangle$. Cette correction est obtenue à l'aide d'un seul modulateur de phase (fig. 2.14).

Génération d'un cluster temporel à l'aide de l'encodage en polarisation

Nous expliquons maintenant comment transcrire les portes *fusion* de type I et II (fig. 2.10-a et b) vers l'encodage temporel mais en utilisant cette fois-ci l'encodage en polarisation pour

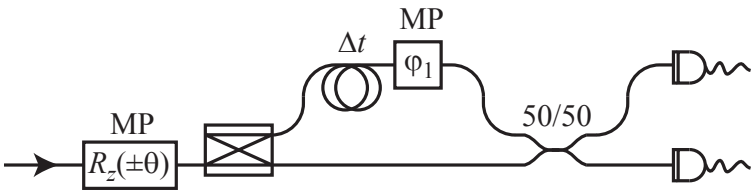

FIGURE 2.13 Circuit optique réalisant les mesures à un qubit nécessaires au traitement à l'aide de l'encodage spatial. Le modulateur de phase applique l'opération $R_z(\pm\theta)$. Le reste du circuit applique la porte Hadamard ($\varphi_1 = 0$) ainsi que la mesure dans la base de calcul $\{|t_0, |t_1\rangle\rangle\}$.

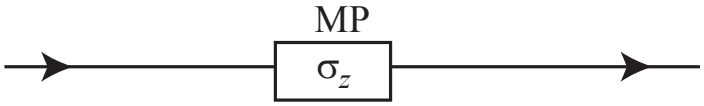

FIGURE 2.14 Circuit implémentant la correction σ_z sur un qubit temporel. Le modulateur de phase applique un changement de phase relatif de π entre les composantes $|t_0\rangle$ et $|t_1\rangle$.

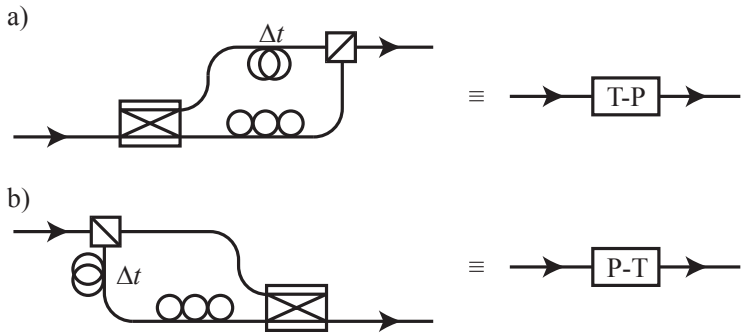

FIGURE 2.15 Conversion de l'encodage. a) Conversion d'un qubit temporel vers un qubit encodé en polarisation. b) Conversion d'un qubit encodé en polarisation vers un qubit temporel.

le traitement. Pour ce faire, il suffit de convertir le qubit temporel en qubit en polarisation à l'aide du circuit de la fig. 2.4 tronqué après le premier cube polariseur, tel que montré à la fig. 2.15-a. Ensuite, on utilise l'équivalent tout-fibre des circuits de la fig. 2.10-a et c pour effectuer la fusion, tel que montré à la fig. 2.16. Finalement, on doit re-convertir vers l'encodage temporel à l'aide du circuit de la fig. 2.15-b.

Traitement à l'aide de l'encodage en polarisation

La façon d'effectuer le traitement à l'aide de la polarisation devrait, à ce point, être évidente. Il suffit de convertir chaque qubit temporel à mesurer vers l'encodage en polarisation

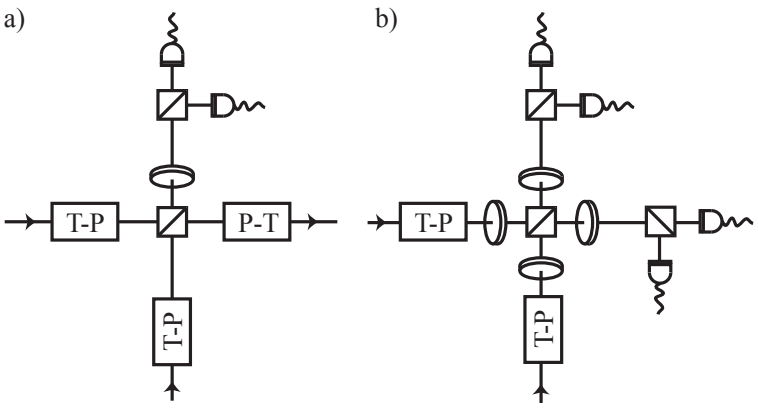

FIGURE 2.16 a) Porte *fusion* de type I à l'aide de l'encodage en polarisation. b) Porte *fusion* de type II à l'aide de l'encodage en polarisation.

et ensuite d'appliquer les opérations désirées à l'aide d'un contrôleur de polarisation et d'un cube polariseur.

2.2.3 Discussion

La technologie requise pour implémenter les circuits présentés ci-haut existe et est présentement disponible. Les composants tout-fibre tels que les coupleurs et les contrôleurs de polarisation ont le mérite d'avoir une perte négligeable. Les composants fibrés, tel le cube polariseur, peuvent aussi être fabriqués avec un perte très faible. Les composants électrooptiques actifs (commutateur optique et modulateur de phase) sont disponibles commercialement à des fréquences de commutation de l'ordre de 10 GHz. Par contre, les pertes de ces composants peuvent excéder 2 dB. Les pertes substantielles résultantes limiteront l'application des circuits proposés à la création de clusters contenant quelques qubits seulement. Par contre, ce problème n'est que technique et il est raisonnable d'espérer une diminution des pertes dans un avenir rapproché. L'autre difficulté inhérente à la réalisation des circuits proposés est celui de la stabilisation des phases des interféromètres. Or, tel que discuté à la section 2.1.4, ce problème peut être éliminé si on réduit suffisamment l'espacement temporel Δt.

Une analyse plus complète est nécessaire. En particulier, l'implémentation des idées présentées ci-haut devra être précédée par une estimation de la probabilité de réussite en fonction de la taille du cluster désiré et en tenant compte de toutes les sources d'imperfection potentielles (pertes optiques, bruit des détecteurs, probabilité de génération des clusters à deux qubits, etc.)

Les résultats présentés dans cette section ont été publiés en 2006 [113]. En 2007, R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaek, T. Jennewein et A. Zeilinger ont

réalisé la première démonstration de principe d'un CQBM avec opérations en aval programmables en 150 ns [81]. Leur approche, basée sur l'encodage en polarisation à l'air libre, ne permet cependant pas de tirer avantage du confinement dans la fibre et de la rapidité des composants électrooptiques fibrés. Les problèmes citées à la section 2.2.1 indiquent que cette approche est irréalisable à grande échelle. Nous croyons que l'approche tout-fibre proposée ici permettra, à long terme, de surmonter certains obstacles et de diminuer le temps nécessaire pour programmer les opérations en aval à quelques nanosecondes ou moins.

Chapitre 3

Sources de paires de photons

La création de qubits photoniques intriqués nécessite deux ingrédients. Le premier est une source de paires de photons et le deuxième est une méthode pour intriquer les qubits encodés à l'aide des degrés de liberté des photons de la paire. Une condition est cependant essentielle pour utiliser ces paires de photons intriqués pour la communication quantique : la probabilité de créer plus d'une paire doit être beaucoup plus faible que celle d'en créer une seule. Autrement, les corrélations quantiques sont difficiles à extraire car il est impossible de séparer les paires une à une. Dans ce chapitre, nous présentons une nouvelle méthode simple et rapide permettant de caractériser une source de paires de photons.

3.1 Théorie de la génération de paires de photons

L'optique non-linéaire est le domaine de l'optique traitant du comportement de la lumière dans un milieu où la réponse de la polarisation diélectrique $P(t)$ est non-linéaire en fonction du champ électrique $E(t)$ de la lumière incidente [114]. Cette non-linéarité s'exprime par la relation

$$P(t) = \epsilon_0 \left[\chi^{(1)}E(t) + \chi^{(2)}E^2(t) + \chi^{(3)}E^3(t) + \ldots\right], \tag{3.1}$$

où ϵ_0 est la permittivité du vide, $\chi^{(1)}$ est la susceptibilité linéaire et $\chi^{(n)}$, où $n > 1$, est la susceptibilité non-linéaire d'ordre n.[1] En communication quantique, seuls les processus non-linéaires de second ou troisième ordre sont, dans la plupart des cas, exploités. Lorsque le champ électrique incident est quasi-monochromatique, la non-linéarité du milieu a pour effet de modifier le contenu spectral de la polarisation et d'y introduire d'autres fréquences que celle du champ incident. Par conséquent, la lumière ré-émise par les dipôles a aussi un contenu spectral modifié.

Nous discuterons uniquement des processus non-linéaires permettant de générer des paires de photons. Historiquement, les premières sources de paires de photons intriqués tiraient profit de transitions atomiques à deux photons [25, 115, 26]. Or, ce processus est tel que les deux photons issus de la relaxation de l'atome sont émis dans des directions indépendantes l'une de l'autre. Par conséquent, il est très difficile de détecter les deux photons simultanément. Malgré

1. En général, la susceptibilité est un tenseur.

cette difficulté, cette approche a quand même permis de réaliser les toutes premières violations du théorème de Bell dans une série d'expériences désormais célèbres [25, 115, 26, 27, 28].

En 1987 et 1988, les travaux de C. K. Hong, L. Mandel et Z. Y. Ou ont pavé la voie vers une nouvelle génération d'expériences basées sur la conversion paramétrique spontanée [116, 117, 118]. Cette approche, utilisée dans les travaux de cette thèse, permet de créer des paires de photons émis dans des directions bien précises, ce qui facilite leur détection. La maîtrise de la conversion paramétrique spontanée est en grande partie responsable des avancées importantes de la communication quantique expérimentale réalisées au cours des quinze dernières années [8]. Une description détaillée de ce processus est présentée à la section 3.1.1. Un autre processus important permettant de générer des paires de photons est le mélange à quatre ondes (M4O) et est discuté à la section 3.1.2.

3.1.1 Conversion paramétrique spontanée

La *conversion paramétrique spontanée* (CPS) est un processus non-linéaire qui dépend de la susceptibilité de second ordre $\chi^{(2)}$ et est un exemple de *mélange à trois ondes* [114]. La CPS est l'analogue quantique de l'amplification paramétrique. Ce processus, décrit par l'optique non-linéaire classique, prédit que lorsqu'un faisceau intense de fréquence ω_p, appelé *faisceau pompe*, est mélangé dans le milieu non-linéaire avec un faisceau d'intensité beaucoup moindre et de fréquence $\omega_s < \omega_p$, appelé *faisceau signal*, alors il est possible, sous certaines conditions, que l'énergie de la pompe soit transférée partiellement vers le signal et dans la création d'un autre faisceau de fréquence $\omega_c = \omega_p - \omega_s$ et appelé *faisceau complémentaire*. Le faisceau signal est donc amplifié. La théorie classique prédit que s'il n'y a pas de faisceau signal au départ, alors l'énergie de la pompe ne peut être transférée.

La quantification du champ électromagnétique permet de traiter la lumière comme un objet quantique composé de photons [119]. La description quantique de l'amplification paramétrique prédit alors que même si le faisceau signal correspond au vide, il est quand même possible qu'un photon de la pompe soit annihilé et converti en un photon signal et un photon complémentaire. L'appellation signal et complémentaire devient alors arbitraire. Cette CPS est parfois interprétée comme une amplification des fluctuations du vide quantique. La première observation de la CPS a été réalisée par D. C. Burnham et D. L. Weinberg en 1970 [120].

Le milieu non-linéaire joue le rôle de médiateur de l'interaction entre les différents faisceaux. Cependant, la CPS est telle qu'elle ne laisse aucune trace dans le milieu et l'énergie et la quantité de mouvement totale des photons sont conservées. Ceci donne lieu aux équations

d'accord de phase :

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_c, \tag{3.2}$$

$$n_p\mathbf{k}_p = n_s\mathbf{k}_s + n_c\mathbf{k}_c, \tag{3.3}$$

où n_p, n_s et n_c sont les indice de réfraction de la pompe, le signal et le complémentaire dans le milieu non-linéaire. Si l'accord de phase n'est pas réalisé, la probabilité de CPS reste négligeable tout au long de la transmission dans le milieu non-linéaire. Dans le cas contraire, les différents faisceaux sont en phase et l'interaction est favorisée. En pratique, les photons générés ne sont pas monochromatiques mais possèdent une largeur spectrale dictée par celle de la pompe et par les propriétés du milieu non-linéaire. Cet accord de phase est possible à réaliser à l'aide de cristaux biréfringents en choisissant bien la polarisation de la pompe par rapport aux axes lent et rapide du cristal. Il existe deux type d'accord de phase. Dans le type I, la polarisation rectiligne de la pompe est orthogonale à celle du signal et du complémentaire. Dans le type II, les polarisations rectilignes de la pompe et du signal sont identiques. De plus, la polarisation du complémentaire est orthogonale à celle du signal (et de la pompe). Ces deux approches ont permis de générer des paires de photons intriqués à maintes reprises [19, 20].

La CPS dans les cristaux biréfringents est un processus très inefficace. La probabilité qu'un photon de pompe soit converti est typiquement de l'ordre de 10^{-10}. De plus, l'accord de phase est dicté par les propriétés des cristaux et le choix est limité. La technique de « poling » périodique [2] de cristaux offre plus de possibilités et une efficacité non-linéaire accrue. Dans cette technique, un champ électrique statique et très intense est appliqué momentanément sur différentes sections d'un cristal afin d'inverser périodiquement, et de façon permanente, le moment dipolaire électrique, tel qu'illustré à la fig. 3.1. Pour un matériau et un pas de réseau Λ donnés, un *quasi-accord de phase* [3] est possible même si l'accord de phase dans chaque section individuelle n'est pas satisfait [114]. De plus, il est possible d'obtenir un quasi-accord de phase lorsque tous les faisceaux sont polarisés dans le même plan que les moments dipolaires du réseau. Dans ce cas, l'éq. 3.3 doit être remplacée par

$$n_p k_p = n_s k_s + n_c k_c + \frac{2\pi}{\Lambda}. \tag{3.4}$$

Dans cette thèse, nous avons utilisé un cristal de niobate de lithium ($LiNbO_3$) polé périodiquement (NLPP). Ce cristal possède trois réseaux aux périodes respectives de 7,05,

2. « Periodic poling ».
3. « Quasi-phase-matching ».

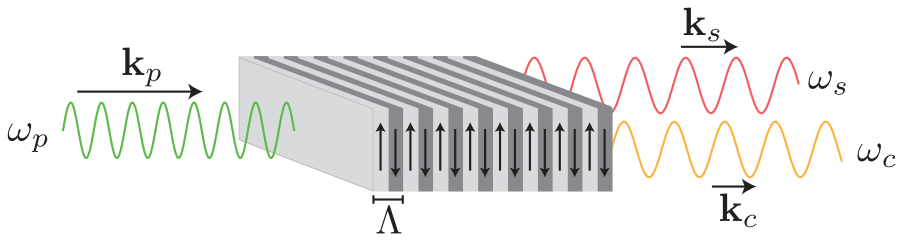

FIGURE 3.1 Cristal « polé » périodiquement. Les flèches indiquent la direction du moment dipolaire électrique permanent. Le pas du réseau est Λ.

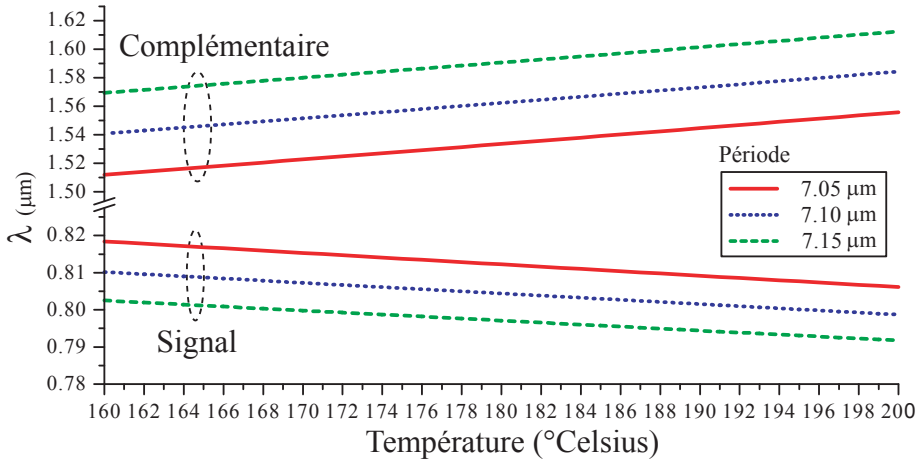

FIGURE 3.2 Quasi-accord de phase dans un cristal de niobate de lithium polé périodiquement pour une pompe à 530,6 nm.

7,10 et 7,15 µm. Le cristal est placé dans un four permettant d'atteindre une température de 200 °C. À l'aide des équations de Sellmeier appliquées au niobate de lithium [121], on peut résoudre les équations de quasi-accord de phase pour une longueur d'onde de pompe donnée (dans notre cas, $\lambda_p = 530{,}6$ nm). Le graphique de la fig. 3.2 montre le résultat. On voit donc qu'en faisant varier la température entre 160 et 200 °C, on peut générer un signal et un complémentaire aux environ de 810 et 1550 nm.

Description quantique de la conversion paramétrique spontanée

Dans le but de bien comprendre les résultats de ce chapitre, nous résumons la description quantique de la CPS. Celle-ci repose sur l'hamiltonien décrivant l'interaction entre la pompe, le signal et le complémentaire durant la transmission dans le milieu non-linéaire [122] :

$$\hat{H} = \hbar\omega_s \hat{s}^\dagger \hat{s} + \hbar\omega_c \hat{c}^\dagger \hat{c} + \hbar\omega_p \hat{p}^\dagger \hat{p} + i\hbar\tilde{\chi}^{(2)}(\hat{s}\hat{c}\hat{p}^\dagger - \hat{s}^\dagger \hat{c}^\dagger \hat{p}) \tag{3.5}$$

où $\hat{s}$, $\hat{c}$ et $\hat{p}$ sont les opérateurs d'annihilation d'un photon signal, complémentaire et de pompe, respectivement, et $\tilde{\chi}^{(2)}$ est égale à $\chi^{(2)}$ à une constante près. Nous appliquerons l'approximation paramétrique dans laquelle la pompe est considérée comme très intense, non appauvrie par l'interaction, monochromatique et dans l'état cohérent $|\alpha \mathrm{e}^{-i\omega_p t}\rangle$, où α est réel. On rappelle que le carré de l'amplitude α^2 correspond au nombre moyen de photons de pompe durant l'intervalle de temps T. Elle est reliée à la puissance crête de la pompe P par

$$P = \frac{\alpha^2 \hbar \omega_p}{T}. \tag{3.6}$$

L'hamiltonien devient alors

$$\hat{H} = \hbar\omega_s \hat{s}^\dagger \hat{s} + \hbar\omega_c \hat{c}^\dagger \hat{c} + \hbar\omega_p \alpha^2 + i\hbar\eta(\mathrm{e}^{i\omega_p t}\hat{s}\hat{c} - \mathrm{e}^{-i\omega_p t}\hat{s}^\dagger \hat{c}^\dagger) \tag{3.7}$$

où $\eta = \tilde{\chi}^{(2)}\alpha$. On passe ensuite à la représentation d'interaction dans laquelle on divise l'hamiltonien en deux parties, $\hat{H} = \hat{H}_0 + \hat{H}_I$, où $\hat{H}_0 = \hbar\omega_s \hat{s}^\dagger \hat{s} + \hbar\omega_c \hat{c}^\dagger \hat{c} + \hbar\omega_p \alpha^2$ et $\hat{H}_I = i\hbar\eta(\mathrm{e}^{i\omega_p t}\hat{s}\hat{c} - \mathrm{e}^{-i\omega_p t}\hat{s}^\dagger \hat{c}^\dagger)$. On obtient alors l'hamiltonien d'interaction

$$\hat{H}'_I = \mathrm{e}^{i\hat{H}_0 t/\hbar} \hat{H}_I \mathrm{e}^{-i\hat{H}_0 t/\hbar} \tag{3.8}$$

que l'on peut simplifier à l'aide de l'identité

$$\mathrm{e}^{x\hat{a}^\dagger \hat{a}} \hat{a} \mathrm{e}^{-x\hat{a}^\dagger \hat{a}} = \hat{a}\mathrm{e}^{-x}, \tag{3.9}$$

où x est un scalaire, et obtenir

$$H'_I = i\hbar\eta \left[\mathrm{e}^{i(\omega_p - \omega_s - \omega_c)t}\hat{s}\hat{c} - \mathrm{e}^{-i(\omega_p - \omega_s - \omega_c)t}\hat{s}^\dagger \hat{c}^\dagger\right]. \tag{3.10}$$

Les facteurs oscillants disparaissent grâce à la conservation de l'énergie : $\omega_p = \omega_s + \omega_c$. L'opérateur d'évolution est donné par

$$\hat{U}'_I(t) = \exp(-i\hat{H}'_I t/\hbar) = \exp[\xi(\hat{s}\hat{c} - \hat{s}^\dagger \hat{c}^\dagger)] \tag{3.11}$$

où t est le temps d'interaction et $\xi = \eta t = \tilde{\chi}^{(2)}\alpha t$. L'opérateur $\hat{U}'_I(t)$ est bien connu : il s'agit de l'opérateur de compression à deux modes spectraux [4] et son application sur l'état vide

4. « Two-mode squeezing operator ».

$|0,0\rangle$ décrit le processus de CPS non-dégénérée. On peut montrer que (cf. [122])

$$\exp[\xi(\hat{s}\hat{c} - \hat{s}^\dagger\hat{c}^\dagger)]|0,0\rangle = \frac{1}{\cosh\xi}\sum_{n=0}^{\infty}(-1)^n(\tanh\xi)^n|n,n\rangle, \tag{3.12}$$

où $|n,n\rangle \equiv |n\rangle_s \otimes |n\rangle_c$ est l'état de Fock à n photons dans le faisceau signal et n photons dans le faisceau complémentaire. La probabilité de créer n paires est donc

$$p_n = \frac{(\tanh\xi)^{2n}}{(\cosh\xi)^2}. \tag{3.13}$$

Le nombre moyen de paires créées, quantité que nous nommons *luminosité* et notons μ, est donnée par

$$\mu \equiv \sum_{n=0}^{\infty} np_n = \sinh^2\xi = \sinh^2(\tilde{\chi}^{(2)}\alpha t). \tag{3.14}$$

Ainsi, on peut écrire p_n comme

$$p_n = \frac{\mu^n}{(1+\mu)^{n+1}}. \tag{3.15}$$

Cette distribution est qualifiée de *thermique* par analogie avec le traitement du corps noir. Dans ce régime, la présence d'une ou plusieurs paires de photons stimule la création d'autres paires.

Lorsque la puissance de pompe est suffisamment faible, on peut négliger les termes $p_{n\geq 2}$ car $\mu \ll 1$ et la probabilité de créer une paire augmente linéairement avec la puissance de pompe :

$$p_1 = \frac{\mu}{(1+\mu)^2} \approx \mu \approx (\tilde{\chi}^{(2)}\alpha t)^2 = \frac{(\tilde{\chi}^{(2)}t)^2 PT}{\hbar\omega_p}, \tag{3.16}$$

où nous avons utilisé l'éq. 3.6.

Quelques précisions sont nécessaires. L'état 3.12 est tel que tous les photons du faisceau signal sont dans le même mode temporel et spatial. Cette condition s'applique pour le faisceau complémentaire. Pour satisfaire cette condition avec une pompe pulsée, il faut que le temps de cohérence des photons générés τ_c soit supérieur à la durée de l'impulsion T. Lorsque la pompe est continue, il faut que le temps de cohérence des photons générés soit supérieur ou égal à celui de la pompe. En général, la largeur spectrale des photons générés par la CPS est grande et cette condition n'est pas satisfaite à moins de filtrer le spectre des photons.

Lorsque la durée de l'impulsion de pompe (ou le temps de cohérence de la pompe lorsqu'elle est continue) est beaucoup plus grande que le temps de cohérence des photons, une multitude processus thermiques peuvent survenir dans plusieurs modes temporels distincts. Le nombre de modes peut être défini comme $N \approx T/\tau_c$ [123]. En diminuant la puissance de

la pompe, la probabilité de créer plus d'une paire par mode temporel devient négligeable. On a alors un ensemble de modes pouvant contenir soit zéro, soit une paire de photons, avec la probabilité de créer une paire par mode égale à $p_1 \approx (\tilde{\chi}^{(2)}t)^2 PT/N\hbar\omega_p \ll 1$. La probabilité de créer n paires dans N modes peut alors être modélisée par une distribution binomiale pour laquelle $p_0 \approx 1 - p_1$ par mode. Or, cette distribution est équivalente à une distribution de Poisson lorsque $p_1 \ll 1$ et N est grand. La probabilité p'_n de créer n paires est alors donnée par

$$p'_n = \frac{\mathrm{e}^{-\mu}\mu^n}{n!}, \tag{3.17}$$

où la luminosité est

$$\mu = Np_1 \approx \frac{(\tilde{\chi}^{(2)}t)^2 PT}{\hbar\omega_p}. \tag{3.18}$$

Comme dans le cas de la distribution thermique, la luminosité augmente linéairement selon la puissance crête de la pompe. On voit également que pour $\mu \ll 1$, $p'_1 \approx p_1$. Dans la même limite, on trouve que $p_2 \approx \mu^2$ et $p'_2 \approx \mu^2/2$, d'où $p_2 \approx 2p'_2$. Ceci s'explique par le fait que pour une source thermique, contrairement à une source suivant la distribution de Poisson, la probabilité d'émettre une deuxième paire de photon est stimulée par la présence de la première. Ceci augmente p_2 au-delà de p'_2.

3.1.2 Mélange à quatre ondes spontané

Une autre approche possible pour générer des paires de photons est de tirer profit de la susceptibilité de troisième ordre ce qui, en général, nécessite un pompage plus intense. Durant les dernières années, beaucoup d'efforts ont été mis dans la création de paires de photons directement dans la fibre optique. Cette approche permet en principe d'éviter les pertes de couplage du cristal vers le cœur de la fibre (pour la transmission et la détection). Les fibres optiques sont faites de verre amorphe. Ainsi, le renversement de la direction du champ électrique $E(t) \to -E(t)$ cause également le renversement de la polarisation : $P(t) \to -P(t)$. L'utilisation de cette condition dans l'éq. 3.1 implique que $\chi^{(2)} = 0$ et qu'on doit exploiter la non-linéarité de troisième ordre pour générer des paires de photons.

Le *mélange à quatre ondes* (M4O) spontané permet cette génération. Lors de ce processus, deux photons de pompe, ayant la même fréquence ou non, sont annihilés pour générer un photon signal et un complémentaire. La description quantique du M4O dégénéré, où les deux photons de pompe sont identiques en fréquence et en polarisation (rectiligne), repose sur l'hamiltonien suivant :

$$\hat{H} = \hbar\omega_s \hat{s}^\dagger \hat{s} + \hbar\omega_c \hat{c}^\dagger \hat{c} + 2\hbar\omega_p \hat{p}^\dagger \hat{p} + i\hbar\tilde{\chi}^{(3)} \left[\hat{s}\hat{c}(\hat{p}^\dagger)^2 - \hat{s}^\dagger \hat{c}^\dagger \hat{p}^2\right], \tag{3.19}$$

où $\tilde{\chi}^{(3)}$ est égale à $\chi^{(3)}$ à une constante près. L'approximation paramétrique nous donne alors le même résultat que l'éq. 3.7 mais avec $\eta = \tilde{\chi}^{(3)}\alpha^2$ et $2\omega_p$ au lieu de $\eta = \tilde{\chi}^{(2)}\alpha$ et ω_p. Le reste du raisonnement est identique à celui de la CPS où l'on aura remplacé $\tilde{\chi}^{(2)}$ par $\tilde{\chi}^{(3)}$, α par α^2 et ω_p par $2\omega_p$. La conséquence directe est que dans la limite où la probabilité de créer plus d'une paire est négligeable, le nombre moyen de paires créées augmente selon le carré de la puissance crête. Ceci est la signature du M4O lorsque $p_{n\geq 2} \ll p_1$ et c'est ce que M. Fiorentino, P. L. Voss, J. E. Sharping et P. Kumar ont observé pour la première fois dans la fibre optique (en 2002) [124].

3.1.3 Ensembles atomiques

Au cours des dernières années, plusieurs groupes ont utilisé l'excitation cohérente d'un ensemble d'atomes (EA) pour générer des paires de photons à partir du processus de *diffusion Raman spontanée*[5] [125, 126, 127, 128]. Un avantage de cette approche est que la largeur spectrale des photons est très étroite, ce qui facilite leur utilisation dans une mesure de Bell [8].

3.1.4 Autocorrélation de second ordre

Une source de paires de photons basée sur la CPS ou le M4O spontané ne peut être décrite par l'optique non-linéaire classique. Il est donc naturel d'établir un critère permettant de prouver ceci expérimentalement. Une approche possible est a été établie en 1956 par R. Hanbury Brown et R. Q. Twiss à l'aide du montage portant désormais leur nom [129] (voir aussi [130]). Ce montage, représenté à la fig. 3.3, a pour but de mesurer les corrélations entre l'intensité instantanée $I(t)$ d'un faisceau à un instant t et celle à un instant $t + \tau$. Plus précisément, supposons que le faisceau est composé de photons et que $I(t)$ est une série d'impulsions séparées dans le temps, chaque impulsion représentant un photon. Selon l'hypothèse de R. Hanbury Brown et R. Q. Twiss, le temps d'émission de chaque photon d'une source quelconque est indépendant de tous les autres. Ainsi, la mesure de la probabilité d'un coup double (détection simultanée de deux photons) aux détecteurs D_A et D_B devrait refléter ceci. Si D_B mesure avec un délai de τ par rapport à D_A, alors la probabilité d'un coup double est donnée par le facteur $\gamma^{(2)}(\tau)$ défini comme

$$\gamma^{(2)}(\tau) = \frac{\langle I(t)I(t+\tau)\rangle}{\langle I(t)\rangle^2} \tag{3.20}$$

$$= \frac{\langle E^*(t)E^*(t+\tau)E(t+\tau)E(t)\rangle}{\langle E^*(t)E(t)\rangle^2} \tag{3.21}$$

5. « Spontaneous Raman scattering ».

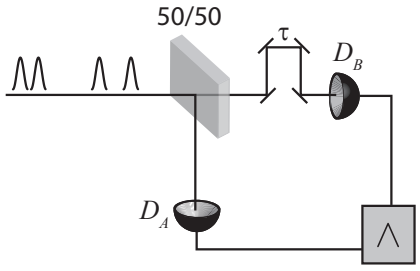

FIGURE 3.3 Montage original de Hanbury Brown et Twiss. 50/50 est une lame séparatrice et $\wedge$ est un compteur de coups doubles (détection simultanée de deux photons).

où $\langle \ldots \rangle$ correspond à moyenne temporelle et $E(t)$ est le champ électrique instantané au temps t. Nous nommons cette quantité *autocorrélation classique de second ordre*. Pour un délai $\tau = 0$ on a $\gamma^2(0) = \langle I(t)^2 \rangle / \langle I(t) \rangle^2$. L'inégalité de Cauchy permet de montrer que [122]

$$1 \leq \gamma^2(0) < \infty \tag{3.22}$$

et que

$$\gamma^2(\tau) \leq \gamma^2(0). \tag{3.23}$$

L'équivalent quantique de l'autocorrélation de second ordre, que nous notons $g^2(\tau)$, est obtenu à l'aide de l'opérateur quantique du champ électrique. Ce dernier est défini comme

$$\hat{E}(t) = \hat{E}^{(+)}(t) + \hat{E}^{(-)}(t), \tag{3.24}$$

où $\hat{E}^{(+)}(t) = iC\hat{a}\mathrm{e}^{-i\omega t}$ est l'opérateur d'annihilation d'un photon au temps t lorsque le champ est unimodal (un seul mode spectral, de polarisation et transverse), $\hat{E}^{(-)}(t) = [\hat{E}^{(+)}(t)]^\dagger$ est l'opérateur de création d'un photon au temps t et C est une constante de normalisation [122]. Ainsi, par analogie avec l'éq. 3.21, on définit

$$g^2(\tau) = \frac{\left\langle \hat{E}^{(-)}(t)\hat{E}^{(-)}(t+\tau)\hat{E}^{(+)}(t+\tau)\hat{E}^{(+)}(t) \right\rangle}{\left\langle \hat{E}^{(-)}(t)\hat{E}^{(+)}(t) \right\rangle \left\langle \hat{E}^{(-)}(t+\tau)\hat{E}^{(+)}(t+\tau) \right\rangle}, \tag{3.25}$$

où $\langle \hat{O} \rangle \equiv \langle \psi | \hat{O} | \psi \rangle$ est la valeur moyenne de l'opérateur $\hat{O}$ dans l'état $|\psi\rangle$. Le numérateur de l'éq. 3.25 est proportionnel à la probabilité P_{AB} de détecter un seul photon à D_A et un seul photon à D_B, $\left\langle \hat{E}^{(-)}(t)\hat{E}^{(+)}(t) \right\rangle$ est proportionnel à la probabilité P_A de détecter un seul photon à D_A et $\left\langle \hat{E}^{(-)}(t+\tau)\hat{E}^{(+)}(t+\tau) \right\rangle$ est proportionnel à la probabilité P_B de détecter un seul photon à D_B avec un délai τ par rapport à D_A. Ainsi, on peut écrire $g^{(2)}(\tau)$ comme

suit :

$$g^{(2)}(\tau) = \frac{P_{AB}}{P_A P_B}. \tag{3.26}$$

Si le temps d'émission de chaque photon est indépendant de tous les autres, alors $P_{AB} = P_A P_B$ et $g^{(2)}(\tau) = 1$.

À l'aide des définitions de $\hat{E}^{(\pm)}(t)$, on peut simplifier l'éq. 3.25 pour obtenir

$$g^{(2)}(\tau) = 1 + \frac{\langle(\Delta\hat{n})^2\rangle - \langle\hat{n}\rangle}{\langle\hat{n}\rangle^2}, \tag{3.27}$$

où $\hat{n} = \hat{a}^\dagger\hat{a}$ est l'opérateur nombre de photon. Pour un état cohérent

$$|\alpha\rangle = \mathrm{e}^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{n!}|n\rangle, \tag{3.28}$$

le nombre de photons suit une distribution de Poisson et par conséquent, $\langle(\Delta\hat{n})^2\rangle = \langle\hat{n}\rangle = \mu$, d'où $g^{(2)}(\tau) = 1$. On en conclut que dans un tel état, qui est l'équivalent quantique d'une onde monochromatique, le temps d'émission de chaque photon est indépendant de tous les autres et ceci satisfait l'hypothèse de Hanbury Brown et Twiss. Une source thermique suivant la distribution 3.13 donne cependant $g^{(2)}(0) = 2$. Ce résultat a été observé pour la première fois par Hanbury Brown et Twiss [129] et était contraire à leur hypothèse initiale. Il s'explique par le fait que pour une telle source, il est plus probable de détecter deux photons au même temps car la création du deuxième est stimulée par la présence du premier. Ce groupement des photons [6] est caractéristique d'une source thermique.

Les corrélations temporelles des états cohérents et les sources thermiques peuvent donc s'expliquer classiquement. Ce n'est plus le cas pour un photon unique dans l'état de Fock $|1\rangle$. En effet, en raison de la nature indivisible du photon, un coup double est impossible et $g^{(2)}(0) = 0$. En fait, un champ est non classique lorsque $0 \leq g^{(2)}(0) < 1$, ce qui constitue le critère recherché.

3.2 Sources de paires de photons et communication quantique

Les sources de paires de photons sont un élément essentiel à l'implémentation de plusieurs protocoles de communication quantique sur grande distance. Par exemple, la distribution quantique de clés (DQC) basée sur l'intrication [55, 56], la téléportation quantique [131] ainsi

6. « Photon bunching ».

que le répéteur quantique [68, 125] nécessitent tous une source de paires de photons. Une autre application intéressante est une *source de photons annoncés* (SPA), obtenue lorsque la détection du photon signal annonce la présence du photon complémentaire, et qui se rapproche d'un source à un photon unique [132].

Les sources de paires de photons basées sur la CPS, le M4O spontané ou sur un ensemble d'atomes sont toutes qualifiées de probabilistes car le nombre moyen de paires émises par unité de temps suit une distribution précise telle que la distribution de Poisson ou la distribution thermique. En communication quantique, plusieurs tâches bénéficient grandement de la connaissance exacte de la luminosité μ. Cela est parfois même nécessaire. Pour la DQC basée sur l'intrication, X. Ma, C.-H. Fred Fung, et H.-K. Lo ont montré que le taux de génération de la clé ainsi que la distance maximale sécuritaire peuvent êtres optimisés simultanément en ajustant correctement la luminosité [133]. Un autre exemple est la DQC basée sur l'utilisation d'une SPA. La sécurité de cette approche dépend directement de la capacité qu'a l'émetteur de déterminer la luminosité de sa source [134, 135, 136, 137]. Finalement, H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden et N. Gisin ont montré que la visibilité d'intrication générée par une mesure dans la base de Bell dépend directement de la luminosité [138].

Déterminer la luminosité d'une source de paires de photons est une tâche non triviale lorsque les canaux de transmission entre la source et les détecteurs comportent des pertes. Ce problème peut être contourné lorsque la transmittance de chaque canal est connu précisément. En pratique, la perte associée au couplage de l'air libre au cœur d'une fibre peut être très difficile à mesurer lorsque l'impulsion ne contient qu'un seul photon. Une façon de faire cette mesure est d'utiliser une impulsion laser intense dont le mode transverse est identique à celui de l'impulsion à un photon, mais comme le mode transverse d'une impulsion à une photon est difficile à caractériser à l'aide d'un détecteur de photon unique, cette approche est généralement imprécise et difficile à implémenter [139, 140, 141]. La luminosité peut aussi être calculée à partir de la mesure directe de l'autocorrélation de second ordre [119], mais cette mesure est basée sur la détection de coups triples (détection simultanée de trois photons [7]) provenant de l'émission simultanée de deux paires de photons et nécessite un temps de mesure généralement très long [128, 142]. Par conséquent, une méthode simple, rapide et précise permettant de mesurer la luminosité d'une source ainsi que les pertes entre la source et les détecteurs est nécessaire.

Dans les sections suivantes, nous proposons une nouvelle méthode ayant les propriétés recherchées. Cette méthode est rapide et efficace car elle repose uniquement sur la détection de coups simples et de coups doubles provenant de l'émission d'une seule paire. La section 3.3 présente un modèle décrivant de façon exacte la statistique des mesures de n'importe quelle

7. « Three-fold coincidence ».

source de paires de photons probabiliste. Nous montrons également comment la luminosité et les pertes des canaux peuvent être calculées précisément. Ensuite, la section 3.4 présente une démonstration expérimentale de la méthode proposée. Nous montrons ensuite à la section 3.5 que la méthode est correcte et précise en comparant la prédiction de la valeur de $g^{(2)}(0)$ d'une SPA obtenue à l'aide de notre méthode à la mesure directe de cette quantité. Cette comparaison est ensuite répétée pour plusieurs valeurs de la luminosité. Finalement, la section 3.6 présente une discussion sur les limitations potentielles de notre modèle lorsque les photons sont corrélés spectralement.

3.3 Modélisation de la statistique des coups d'une source de paires de photons

3.3.1 Description du modèle

Nous avons développé un modèle décrivant de la statistique des coups du montage de la fig. 3.4. Ce modèle est exact car aucune approximation n'est nécessaire. Cette construction a pour but de calculer les éléments du vecteur d'état $\mathbf{P}$ de l'éq. 3.29 et qui décrit la probabilité

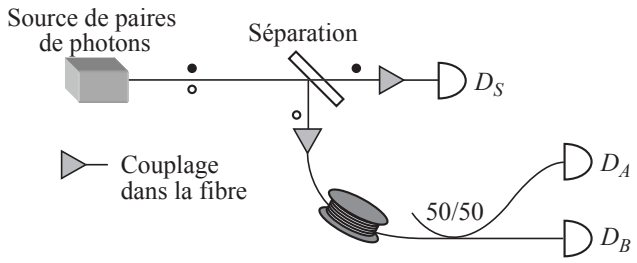

FIGURE 3.4 Les sources modélisées sont de nature probabiliste. Ceci inclut les sources basées sur la CPS dans les cristaux, le M4O spontané dans la fibre optique et les ensembles d'atomes. La distribution du nombre de paires émises durant la fenêtre de mesure est donnée par une distribution arbitraire mais est supposée être connue. Les photons de chaque paire sont séparés spatialement, soit par génération non colinéaire ou par un miroir dichroïque lorsque les faisceaux signal et complémentaire sont non dégénérés et colinéaires, et transmis dans leur canal respectif. Chaque faisceau est filtré pour éliminer la pompe résiduelle et les paires sont couplées dans la fibre. Les photons du faisceau signal sont détectés par le détecteur D_S, ce qui permet d'annoncer la présence d'un photon complémentaire. Le faisceau complémentaire est incident sur une séparatrice 50/50 et les sorties sont envoyées vers les détecteurs D_A et D_B. Nous supposons que les détecteurs sont incapables de résoudre le nombre de photons.

de trouver les détecteurs D_S, D_A et D_B dans un état donné :

$$\mathbf{P} = \left(P_{\bar{A}\bar{B}\bar{S}}\ P_{A\bar{B}\bar{S}}\ P_{\bar{A}B\bar{S}}\ P_{\bar{A}\bar{B}S}\ P_{AB\bar{S}}\ P_{A\bar{B}S}\ P_{\bar{A}BS}\ P_{ABS} \right)^{\mathrm{T}}, \tag{3.29}$$

où T dénote le transposé du vecteur ligne. Plus précisément, chaque élément de $\mathbf{P}$ décrit la probabilité qu'un sous-ensemble de détecteurs aient détectés un coup durant la *fenêtre de mesure*. Cette dernière est définie comme l'intervalle de temps durant lequel les coups sont compilés dans l'analyse statistique. Par exemple, $P_{A\bar{B}\bar{S}}$ est la probabilité qu'un coup simple soit enregistré à D_A durant la fenêtre de mesure, P_{ABH} est la probabilité qu'un coup triple soit enregistré aux trois détecteurs durant la fenêtre de mesure, etc. L'objectif de la méthode est de déterminer comment le vecteur $\mathbf{P}$, se trouvant initialement dans l'état $\mathbf{P}_0 = \left(1\ 0\ \ldots\ 0 \right)^{\mathrm{T}}$, évolue lorsque une ou plusieurs paires sont incidentes sur les détecteurs durant la fenêtre de mesure. Premièrement, nous décrivons l'effet d'un seule paire à l'aide de la matrice de transition suivante :

$$M_\eta = \begin{pmatrix} (1-\eta_S)(1-\eta_A-\eta_B) & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \eta_A(1-\eta_S) & (1-\eta_B)(1-\eta_S) & 0 & 0 & 0 & 0 & 0 & 0 \\ \eta_B(1-\eta_S) & 0 & (1-\eta_A)(1-\eta_S) & 0 & 0 & 0 & 0 & 0 \\ \eta_S(1-(\eta_A+\eta_B)) & 0 & 0 & 1-(\eta_A+\eta_B) & 0 & 0 & 0 & 0 \\ 0 & \eta_B(1-\eta_S) & \eta_A(1-\eta_S) & 0 & 1-\eta_S & 0 & 0 & 0 \\ \eta_A\eta_S & \eta_S(1-\eta_B) & 0 & \eta_A & 0 & 1-\eta_B & 0 & 0 \\ \eta_B\eta_S & 0 & \eta_S(1-\eta_A) & \eta_B & 0 & 0 & 1-\eta_A & 0 \\ 0 & \eta_B\eta_S & \eta_A\eta_S & 0 & \eta_S & \eta_B & \eta_A & 1 \end{pmatrix}. \tag{3.30}$$

Les éléments de la matrice sont exprimés en fonction de la transmittance totale de chaque canal, notées η_S, η_A et η_B et définies comme la probabilité qu'un photon émis par la source soit détecté par le détecteur respectif à chaque canal. Les pertes incluses dans ces transmittances comprennent toutes les pertes optiques, ce qui comprend le couplage dans la fibre et la séparatrice 50/50, ainsi que la perte relative au rendement quantique imparfait des détecteurs. Chaque élément de M_η décrit la probabilité qu'une paire cause une transition de l'état conjoint des détecteurs. Par exemple, l'élément $M_\eta(1,1)$ correspond à la probabilité que les détecteurs passent de l'état $\bar{A}\bar{B}\bar{S}$ à $\bar{A}\bar{B}\bar{S}$ (autrement dit, rien ne change), qui est égale à la probabilité que le photon signal ne soit pas détecté par D_S, $(1-\eta_S)$, multiplié par la probabilité que le photon complémentaire ne soit détecté ni en D_A, ni en D_B, $(1-\eta_A-\eta_B)$, d'où $M_\eta(1,1) = (1-\eta_S)(1-\eta_A-\eta_B)$. De la même façon, l'élément $M_\eta(2,1)$ est la probabilité de passer de l'état $\bar{A}\bar{B}\bar{S}$ à l'état $A\bar{B}\bar{S}$, qui est donnée par $\eta_A(1-\eta_S)$. Les éléments de la diagonale supérieure sont égaux à 0 car les transitions sont unidirectionnelles et irréversibles (D_A peut passer de l'état $\bar{A}$ à l'état A mais le contraire est impossible, etc.) Les autres éléments de la matrice sont construits selon le même raisonnement. Comme la probabilité totale doit être conservée, la somme des éléments de chaque colonne de M_η est égale à 1. Le vecteur d'état final lorsque une paire est incidente est $M_\eta\mathbf{P}_0$.

Un des avantages de ce formalisme est que la généralisation au cas où i paires sont incidentes est très simple car la transmission de chaque paire dans les canaux est indépendante des autres. Ainsi, i paires produisent le vecteur d'état $(M_\eta)^i\mathbf{P}_0$.

Pour être complet, notre modèle doit également tenir compte des coups sombres dont la cause est autre que les photons provenant de la source.[8] Ceci est fait en construisant une autre matrice M_{cs} en suivant les mêmes règles que pour la matrice M_η. En notant c_S, c_A et c_B les probabilités d'un coup sombre de chaque détecteur durant la fenêtre de mesure, on obtient la matrice M_{cs} suivante :

$$M_{\text{cs}} = \begin{pmatrix} (1-c_A)(1-c_B)(1-c_S) & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ c_A(1-c_B)(1-c_S) & (1-c_B)(1-c_S) & 0 & 0 & 0 & 0 & 0 & 0 \\ (1-c_A)c_B(1-c_S) & 0 & (1-c_A)(1-c_S) & 0 & 0 & 0 & 0 & 0 \\ (1-c_A)(1-c_B)c_S & 0 & 0 & (1-c_A)(1-c_B) & 0 & 0 & 0 & 0 \\ c_Ac_B(1-c_S) & c_B(1-c_S) & c_A(1-c_S) & 0 & 1-c_S & 0 & 0 & 0 \\ c_A(1-c_B)c_S & (1-c_B)c_S & 0 & c_A(1-c_B) & 0 & 1-c_B & 0 & 0 \\ (1-c_A)c_Bc_S & 0 & (1-c_A)c_S & (1-c_A)c_B & 0 & 0 & 1-c_A & 0 \\ c_Ac_Bc_S & c_Bc_S & c_Ac_S & c_Ac_B & c_S & c_B & c_A & 1 \end{pmatrix}. \tag{3.31}$$

Lorsque le nombre de paires émises est inconnu, le vecteur d'état final $\mathbf{P}$ est donné par

$$\mathbf{P} = \sum_{i=0}^{\infty} p_i M_{\text{cs}} (M_\eta)^i \mathbf{P}_0, \tag{3.32}$$

où p_i est la probabilité de créer i paires durant la fenêtre de mesure. Cette équation d'évolution est valide pour n'importe quelle distribution p_i, mais cette dernière est supposée connue. On note que toutes les matrices commutent et l'ordre dans laquelle est sont appliquées sur $\mathbf{P}_0$ est sans importance. La construction des matrices nous assure que chaque élément de $\mathbf{P}$ est compris dans l'intervalle $[0, 1]$ et que la somme des éléments de $\mathbf{P}$ est égale à 1. La probabilité totale est donc conservée. Ce modèle est exact est aucune approximation n'a été nécessaire.

3.3.2 Calcul de la transmittance de chaque canal

Nous montrons ici comment on peut déterminer précisément les grandeurs de μ, η_S, η_A et η_B en ne comptabilisant que les coups simples et les coups doubles résultants de l'émission d'une seule paire. Pour réaliser cette mesure, la puissance de la pompe doit être réduite jusqu'à ce que la probabilité d'émission simultanée de plusieurs paires soit négligeable : $p_i \ll p_1$ où $i > 1$. En pratique, on peut s'assurer que c'est le cas en observant le niveau de corrélation entre les détections à D_S et D_A. Ce niveau de corrélation peut être quantifié par la quantité

$$G = \frac{P_{AS}}{P_S P_A}, \tag{3.33}$$

8. Dans le cas présent, ces coups sombres proviennent de l'excitation thermique de porteurs de charge dans la région d'avalanche des photodiodes utilisées.

où $P_S = P_{\bar{A}\bar{B}S} + P_{A\bar{B}S} + P_{\bar{A}BS} + P_{ABS}$ est la probabilité d'un coup au détecteur D_S durant la fenêtre de mesure, $P_A = P_{A\bar{B}\bar{S}} + P_{A\bar{B}S} + P_{AB\bar{S}} + P_{ABS}$ est la probabilité d'un coup à D_A et $P_{AS} = P_{A\bar{B}S} + P_{ABS}$ est la probabilité d'un coup double à D_A et D_S. Le modèle décrit par l'éq. 3.32 prédit que, pour une distribution de Poisson ou thermique, la quantité G est égale à 1 lorsque la luminosité est très faible et que, en conséquence, les coups doubles sont causés principalement par un coup sombre à D_S et un autre à D_A. Dans la limite opposée où la luminosité est très grande et que les coups doubles sont causés principalement par la détection de photons provenant de l'émission de plusieurs paires, les corrélations entre les coups à D_S et D_A disparaissent et on obtient $G = 1$ à nouveau. Entre ces deux cas limites, G peut atteindre une valeur nettement supérieure à 1 car la probabilité d'émission de plusieurs paires est négligeable devant celle d'émission d'une seule paire.

Nous montrons maintenant comment la mesure de G permet d'obtenir une borne supérieure sur la valeur de la luminosité μ. Ceci se fait en quatre temps.

1. Premièrement, on mesure les probabilités de coup sombre c_S et c_A durant la fenêtre de mesure correspondante.
2. Deuxièmement, on réduit la puissance de la pompe jusqu'à l'obtention d'une valeur de G considérablement supérieure à 1.
3. Troisièmement, un graphique de G en fonction de μ peut être produit en supposant que le couplage dans la fibre est parfait et que les pertes optiques sont nulles. Autrement dit, les transmittances η_S and η_A sont supposées êtres égales au rendement quantique de détection de chaque détecteur.
4. Quatrièmement, une borne supérieure de μ est obtenue de ce graphique en identifiant la plus grande valeur de μ produisant la valeur de G mesurée.

La méthode repose sur le fait que pour une valeur de μ donnée, la réduction des transmittances a pour effet d'abaisser la valeur de G vers 1. Ainsi, la réelle valeur de μ doit être inférieure à celle trouvée à la quatrième étape car les transmittances utilisées sont surestimées. Cette borne inférieure permet ensuite d'obtenir une borne inférieure pour le rapport

$$r = \frac{p_1}{p_{i>1}} \tag{3.34}$$

entre p_1, la probabilité qu'une seule paire soit émise, et $p_{i>1} = 1 - p_0 - p_1$, la probabilité que plus d'une paires soient émises. En guise d'exemple, prenons $\eta_S = 60\%$ et $\eta_A = 25\%$, ce qui correspond au rendement quantique de nos détecteurs, et $c_A = 2.87 \times 10^{-4}$ et $c_S = 2.5 \times 10^{-7}$, ce qui correspond à la probabilité d'un coup sombre de nos détecteurs par fenêtre de mesure de 5 ns. En supposant que la source suit une distribution de Poisson, on obtient la ligne continue de la fig. 3.5.

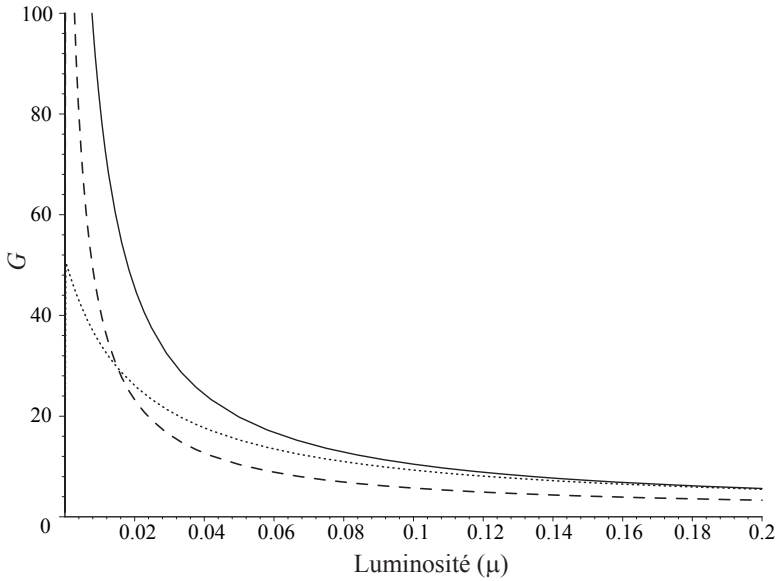

FIGURE 3.5 Niveau de corrélation G en fonction de la luminosité μ. La courbe continue correspond à $\eta_S = 60\%$ et $\eta_A = 25\%$. Elle atteint son extremum lorsque μ est très petit et décroît rapidement vers 1 pour $\mu = 0$ (non visible sur la courbe). La courbe pointillée correspond aux valeurs mesurées de η_S et η_A (cf. section 3.5). La courbe tiretée est calculée avec un coefficient de corrélations spectrales $c = 0{,}5$ (cf. section 3.6).

Lorsque la puissance de pompe est ajustée correctement et que la valeur du rapport r est jugée être suffisamment élevée, l'éq. 3.32 peut être tronquée au premier ordre. À l'aide de cette équation, on peut montrer que la probabilité d'un coup à D_S causé par un photon (et non par une excitation thermique) est donnée par $P_S^{(1)} = (P_S - c_S)/(1 - c_S)$. De la même manière, on trouve que $P_A^{(1)} = (P_A - c_A)/(1 - c_A)$. Finalement, il est possible d'exprimer η_S, η_A et p_1 en fonction de valeurs pouvant être mesurées expérimentalement :

$$\eta_S = \frac{P_{AS} - P_S^{(1)} c_A(1 - c_S) - P_A^{(1)} c_S(1 - c_A) - c_A c_S}{P_A^{(1)}(1 - c_A)(1 - c_S)}, \tag{3.35}$$

$$\eta_A = \frac{P_{AS} - P_S^{(1)} c_A(1 - c_S) - P_A^{(1)} c_S(1 - c_A) - c_A c_S}{P_S^{(1)}(1 - c_A)(1 - c_S)}, \tag{3.36}$$

$$p_1 = \frac{P_S^{(1)}}{\eta_S} = \frac{P_A^{(1)}}{\eta_A}. \tag{3.37}$$

Pour être valide, les mesures de P_{AS}, P_A et P_S doivent être faites dans le régime où la probabilité d'émission de plus d'une paire est négligeable. La procédure pour obtenir η_B est similaire.

La validité de la procédure décrite ci-haut ne repose que sur une seule condition : il doit

être physiquement possible de réduire la probabilité d'émission de plusieurs paires de la source à un niveau négligeable. Par exemple, ceci peut être fait en utilisant la mesure de G. Par contre, la détermination de la luminosité nécessite la connaissance préalable de la relation entre p_1 et μ. Lorsque la source suit une distribution de Poisson, on a $p_1 = \mu \exp(-\mu)$. Dans le cas d'une distribution thermique, on a $p_1 = \mu/(1+\mu)^2$.

Lorsque les transmittances sont connues précisément, on peut utiliser l'éq. 3.32 pour calculer la luminosité correspondant à n'importe quelle valeur de la probabilité d'annonce P_S, un paramètre qui est facile à mesurer expérimentalement. Ceci permet aussi de prédire la valeur de tous les éléments du vecteur $\mathbf{P}$ en fonction de P_S. On remarque finalement que notre méthode ne nécessite pas la connaissance de la grandeur de la susceptibilité non-linéaire du milieu.

3.3.3 Application à une source de photons annoncés

La connaissance de la transmittance de chaque canal ainsi que la nature de la source peuvent être utilisées pour prédire la valeur de l'autocorrélation de second ordre du faisceau complémentaire pour n'importe quelle valeur de la probabilité d'annonce P_S. La distribution du nombre de photons dans le faisceau complémentaire est égale à la distribution du nombre de paires mais avec une composante p_0 réduite grâce à l'annonce fournie par le faisceau signal. Tel que discuté à la section 3.1.4, une mesure donnant $g^{(2)}(0) < 1$ signifie que la source est non classique.

Pour démontrer que notre modèle est juste, nous avons comparé prédictions et mesures directes de $g^{(2)}(0)$. Dans cette expérience, qui peut être vue comme la mesure d'un sous-ensemble de l'éq. 3.32, les détecteurs D_A et D_B sont activés uniquement quand D_S enregistre un coup. Pour cette comparaison, nous avons utilisé une définition de l'autocorrélation de second-ordre légèrement différente de la définition formelle de l'éq. 3.25. Cette définition opérationnelle est

$$g^{(2)}(0) = \frac{P_{AB|S}}{P_{A|S} \times P_{B|S}}, \tag{3.38}$$

où $P_{AB|S}$ est la probabilité d'un coup double à D_A et D_B conditionnel à un coup à D_S, etc. Contrairement à la définition formelle de $g^{(2)}(0)$, les coups ne sont pas causés uniquement par un seul photon. Cela est nécessaire car un détecteur sans bruit capable de résoudre le nombre de photons avec certitude n'existe pas. L'autre différence est la fenêtre de mesure utilisée pour évaluer les probabilités. Celle de la définition formelle est infiniment courte et nécessiterait un détecteur ayant une résolution temporelle du même ordre. Cela est impossible et en pratique les probabilités sont évaluées durant la fenêtre de mesure implicite à la définition opérationnelle. Malgré cela, la pertinence de la définition opérationnelle n'est pas mise en

cause car elle est équivalente à la définition formelle lorsque la probabilité d'émission de plusieurs paires durant la fenêtre de mesure est suffisamment faible et que les coups sombres sont négligeables. Heureusement, les conditions dans lesquelles une source de photons annoncés est utilisée se rapprochent de ce cas idéal.

Pour une probabilité d'annonce p_S donnée, il est possible de mesurer directement la valeur de $g^{(2)}(0)$ à l'aide du montage de la fig. 3.4 en ne compilant que les événements où un coup est enregistré à D_S. D'autre part, la valeur de $g^{(2)}(0)$ correspondante à la probabilité d'annonce donnée peut être prédite à l'aide de l'éq. 3.32. Les résultats expérimentaux sont présentés à la section suivante.

Un fait intéressant ressort de notre modèle. Lorsque la source suit une distribution de Poisson et que les coups sombres sont négligeables, l'éq. 3.32 permet de montrer que $g^{(2)}(0) = \mu(2-\eta_S)$. Ceci suggère que pour une source de photons annoncés, la transmittance η_S affecte directement la valeur de $g^{(2)}(0)$ et est un paramètre important à maximiser.

Notons ici que la séparatrice 50/50 du montage de la fig. 3.4 n'est pas nécessaire pour déterminer la luminosité et les transmittances de la source. En effet, seuls D_S et D_A sont nécessaires. La séparatrice et D_B ont été ajoutés uniquement dans le but de vérifier la validité des prédictions du modèle par la mesure directe de $g^{(2)}(0)$. Le vecteur d'état $\mathbf{P}$ ainsi que les matrices M_η et M_{cs} peuvent être facilement modifiés pour décrire un montage sans la séparatrice et le détecteur D_B.

3.4 Montage expérimental

Le montage expérimental est illustré à la fig. 3.6. L'horloge déclenche une diode laser pulsée (modèle PicoTA de PicoQuant) créant des impulsions de 50 ps à 530,6 nm produites par doublage de fréquence d'impulsions à 1061,2 nm. Les impulsions pompent ensuite un cristal de niobate de lithium « polé » périodiquement NLPP (de Stratophase) ayant un pas de réseau $\Lambda = 7{,}05$ µm et chauffé à 175,7 °C à l'aide d'un régulateur de température. Lorsque la CPS survient, un photon signal centré à 811,7 nm accompagné d'un photon complémentaire centré à 1532,2 nm sont créés dans dans le même mode spatial que la pompe (la génération est colinéaire). Les faisceaux sont ensuite séparés à l'aide d'un miroir dichroïque MD. La pompe à 530,6 nm résiduelle est filtrée à l'aide de filtres colorés passe-haut est chaque faisceau est couplé dans une fibre unimodale SMF28 de Corning.

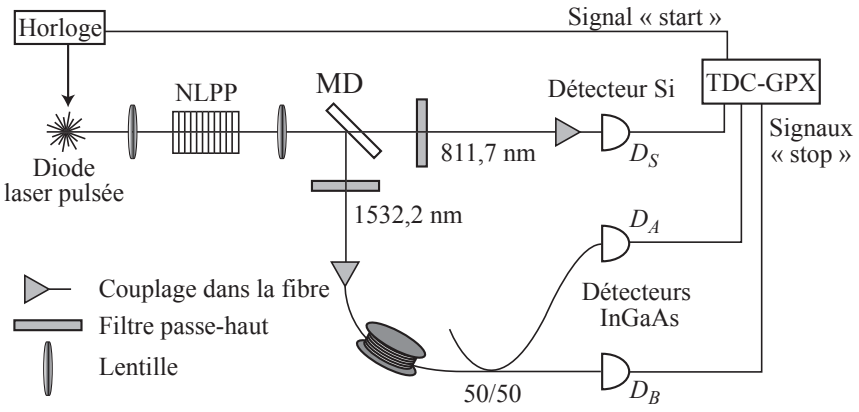

FIGURE 3.6 Montage expérimental de caractérisation d'une source de paire de photons. Une diode laser pulsée pompe un cristal NLPP. Les photons de chaque paire sont séparés à l'aide du miroir dichroïque MD. Les coups aux détecteurs D_S, D_A et D_B sont enregistrés par le convertisseur analogique-numérique temporel TDC-GPX.

3.4.1 Largeur spectrale et temps de cohérence des photons

La longueur d'onde et la largeur spectrale des photons du faisceau signal ont été mesurées directement. Pour ce faire, le faisceau signal est envoyé dans un monochromateur dont la sortie est envoyée dans un détecteur de photon au silicium (voir la section suivante). En balayant le monochromateur, ajusté à sa résolution maximale (inférieure au nm), nous avons obtenu le graphique de la fig. 3.7. Le lissage gaussien de cette courbe nous donne une longueur d'onde centrale de 811,7 nm et une largeur à mi-hauteur de 1,5 nm. En supposant une pompe monochromatique, on en déduit une longueur d'onde centrale de 1532,2 nm est une largeur spectrale de 5,3 nm pour le faisceau complémentaire.

Afin d'obtenir une valeur pour la longueur de cohérence des photons, nous adoptons la définition de Mandel et Wolf ([119], chap. 4) pour laquelle on peut montrer que pour une impulsion gaussienne « Fourier-limitée », la largeur spectrale σ_λ et le temps de cohérence τ_c sont reliés par $\sigma_\lambda \tau_c = \lambda^2/4\pi c$. La largeur spectrale σ_λ est reliée à la largeur à mi-hauteur du spectre $\Delta\lambda$ selon $\Delta\lambda = 2\sqrt{2\ln 2}\sigma_\lambda$. Au final, on a

$$\tau_c = \sqrt{\frac{\ln 2}{2}}\frac{\lambda^2}{\pi c \Delta\lambda}. \tag{3.39}$$

On obtient donc $\tau_c = 0{,}27$ ps pour les photons du faisceau signal et du faisceau complémentaire. Comme τ_c est beaucoup plus petite que la durée des impulsions de la pompe (50 ps), on a l'assurance que notre source est adéquatement décrite par une distribution de Poisson car le nombre de modes temporels dans lesquelles la CPS peut survenir est environ égal à

$50/0{,}27 \approx 185$.

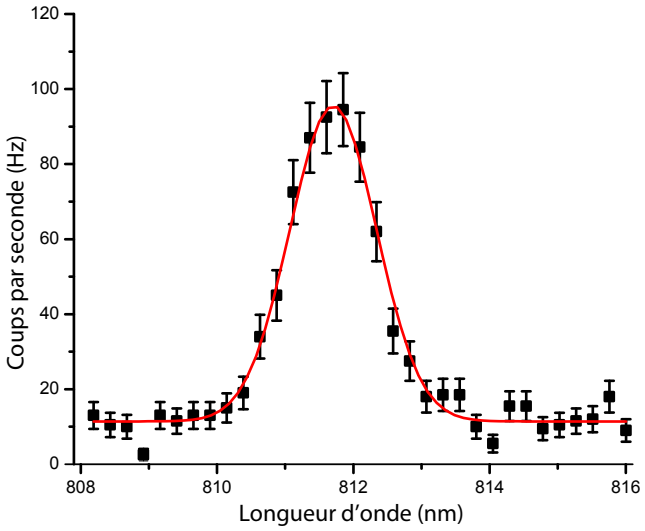

FIGURE 3.7 Spectre du faisceau signal.

3.4.2 Détection

Les photons du faisceau signal sont détectés à l'aide d'une photodiode à avalanche au silicium D_S (modèle SPCM-AQR-14-FC de PERKIN-ELMER) opérée en mode Geiger avec circuit d'étouffement actif[9]. Ce mode d'opération est tel que D_S est continuellement armé pour enregistrer un coup. Lorsque celui-ci survient, le détecteur est désactivé pendant 40 ns pour permettre le ré-armement et éliminer le re-déclenchement.[10] Il possède un rendement quantique d'environ 60% à 800 nm et le taux de coups sombres est d'environ 50 Hz. Après être couplé dans la fibre, le faisceau complémentaire est incident sur un coupleur 50/50. Les branches de sorties sont envoyées vers les détecteurs D_A et D_B (modèle id201 de ID-QUANTIQUE). Ces derniers utilisent une photodiode à avalanche InGaAs opérée en mode Geiger avec activation externe. Par exemple, l'activation de D_A est déclenchée par un signal externe et dure 5 ns. Cette fenêtre d'activation est centrée sur le temps d'arrivée d'un photon complémentaire. Pour éviter le re-déclenchement, un coup est toujours suivi par un temps mort de 10 µs durant lequel le détecteur ne peut être activé de nouveau. Le détecteur est également équipé d'une sortie « gate-out » qui répète le signal d'activation externe du détecteur uniquement si celui-ci n'est pas à l'intérieur d'un temps mort. Le rendement quantique de ces détecteurs peut être ajusté entre 10 et 25%. La probabilité d'un coup sombre

9. « Active quenching circuit ».
10. « Afterpulsing ».

durant une activation de 5 ns est de l'ordre de 10^{-4}. Une description détaillée du fonctionnement de ces détecteurs est disponible dans la référence [143].

3.4.3 Acquisition des données

Les données sont enregistrées à l'aide d'un convertisseur analogique-numérique temporel [11] (modèle TDC-GPX de ACAM). Cet appareil mesure le temps écoulé entre un signal « start », fourni par l'horloge, et plusieurs signaux « stop », fournis par D_S, D_A et D_B. Lorsque un ou plusieurs signaux « stop » sont générés, les intervalles mesurés sont transférés à un ordinateur et traitées en temps réel à l'aide d'un programme C++ conçu spécialement pour cette expérience. Ainsi, chaque coup d'horloge, fourni par un générateur de délais SRS-535 de Stanford Research, résulte en la génération d'une impulsion laser et démarre le convertisseur. La fenêtre de mesure choisie est de 5 ns. Ainsi, les coups à D_S ne sont comptabilisés que s'ils se trouvent à l'intérieur d'une fenêtre de 5 ns centrée sur le temps d'arrivée des photons du faisceau signal. L'horloge est également utilisée pour activer les détecteurs D_A et D_B durant une fenêtre de 5 ns centrée sur le temps d'arrivée des photons du faisceau complémentaire. Pour éviter que le temps mort ne biaise les résultats, les signaux « gate-out » de D_A et D_B sont également enregistrés. Seules les fenêtres de mesure où les deux signaux « gate-out » sont présents sont prises en compte dans les calculs. Comme le taux de transfert des données entre convertisseur et l'ordinateur est limité, la fréquence de répétition de l'horloge est fixée à 30 kHz pour éviter tout débordement des données.

3.5 Résultats expérimentaux

Nous avons d'abord mesuré les probabilités [12] de coup sombre par fenêtre de mesure de 5 ns et obtenu $c_A = 2{,}87 \times 10^{-4}$, $c_B = 3{,}84 \times 10^{-4}$ et $c_S = 2{,}5 \times 10^{-7}$. L'incertitude sur ces probabilités est obtenue en supposant une distribution binomiale des coups. Ensuite, nous avons abaissé la puissance de pompe à l'aide de filtres neutres dans le but d'augmenter le niveau de corrélation entre D_S et D_A jusqu'à l'atteinte de la valeur $G = P_{AS}/(P_A P_S) = 20{,}6 \pm 1{,}0$. La probabilité d'annonce correspondante était $P_S = 0{,}287 \pm 0{,}001\%$. L'intersection de cette valeur avec la ligne continue de la fig. 3.5 nous donne une luminosité $\mu \leq 0{,}0480 \pm 0{,}0013$ et un rapport $r = p_1/p_{i>1} \geq 41{,}0 \pm 2{,}2$, ce que nous avons considéré comme suffisamment élevé. Ensuite, nous avons mesuré les probabilité de coups simples et doubles desquelles nous avons obtenu les résultats suivants : $\eta_S = 0{,}1212 \pm 0{,}0031$, $\eta_A = 0{,}0145 \pm 0{,}0005$,

11. « Time-digital-converter ».

12. Dans cette thèse, « mesurer une probabilité » voudra systématiquement dire « faire une mesure qui permet d'estimer une probabilité ».

$\eta_B = 0{,}0162 \pm 0{,}0005$, $\mu = 0{,}02375 \pm 0{,}00016$ et $r = 83{,}5 \pm 0{,}6$. La courbe de G correspondant à ces transmittances est représentée par la ligne pointillée de la fig. 3.5. La valeur de G correspondant à $\mu = 0{,}02375 \pm 0{,}00016$ est $23{,}9 \pm 0{,}5$, ce qui près de la valeur mesurée (20,6). L'incertitude sur ces valeurs est obtenue avec un calcul de propagation des erreurs.

À l'aide des transmittances obtenues et de l'éq. 3.32, nous avons produit un graphique des valeurs de $P_{AB|S}$, $P_{A|S}$ and $P_{B|S}$ prédites par le modèle pour plusieurs valeurs de la probabilité d'annonce P_S. Ces prédictions sont comparées aux valeurs mesurées sur la fig. 3.8.

Ensuite, nous avons comparé prédictions et mesures de $g^{(2)}(0)$ à la fig. 3.9-a. Ce même graphique montre également la luminosité correspondant à chaque valeur P_S utilisée. Dans tous les cas, l'accord entre prédictions et mesures est excellent.

On notera que pour la mesure directe de $g^{(2)}(0)$, le taux de répétition de l'horloge a été augmenté à 5 MHz et que les détecteurs InGaAs D_A et D_B étaient activés pendant 5 ns uniquement lorsqu'un coup à D_S survenait durant une fenêtre de 5 ns synchronisée avec l'horloge. La fréquence d'activation de D_A et D_B était alors de l'ordre de 30 kHz, mais le temps de chaque activation était aléatoire. Encore une fois, seules les fenêtres de mesure où les deux signaux « gate-out » étaient présents ont été prises en compte.

Notre méthode permet de réduire de façon drastique le temps nécessaire pour caractériser une source car elle est basée uniquement sur la comptabilisation de coups simples et de coups doubles. Ceux-ci sont ensuite utilisés pour déterminer la luminosité μ et le facteur $g^{(2)}(0)$

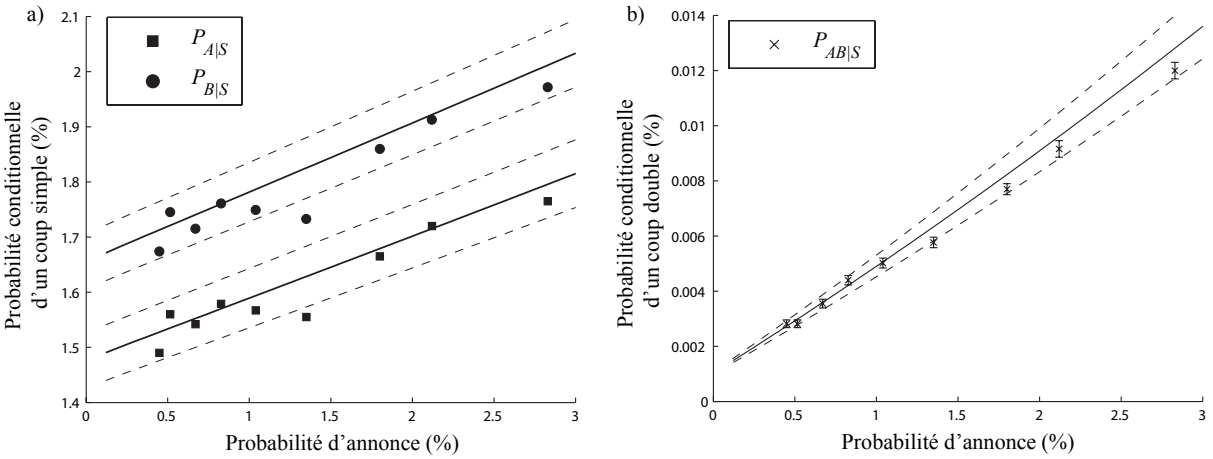

FIGURE 3.8 a) Valeurs prédites (lignes continues) et mesurées (points expérimentaux) des probabilités conditionnelles d'un coup simple $P_{A|S}$ and $P_{B|S}$ en fonction des probabilité d'annonce P_S mesurées. b) Valeurs prédites (ligne continue) et mesurées (points expérimentaux) de la probabilité conditionnelle d'un coup double $P_{AB|S}$. Les lignes tiretées correspondent aux bornes supérieures et inférieures des prédictions obtenues lorsque l'incertitude des transmittances est prise en compte dans le calcul des prédictions.

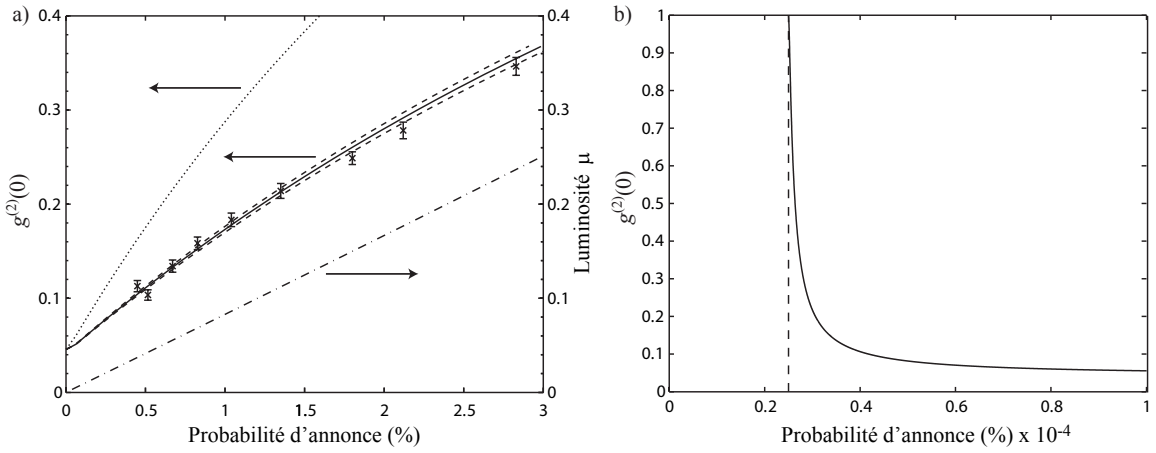

FIGURE 3.9 a) Valeurs prédites de $g^{(2)}(0)$ pour une distribution de Poisson (ligne continue) et une distribution thermique (ligne pointillée), valeurs mesurées (points expérimentaux) ainsi que la luminosité (ligne pointillée-tiretée) en fonction de la probabilité d'annonce mesurée P_S. Les valeurs mesurées sont en excellent accord avec une distribution de Poisson. Les lignes tiretées correspondent aux bornes inférieures et supérieures des prédictions obtenues en tenant compte des incertitudes sur les transmittances. b) En diminuant progressivement la probabilité d'annonce jusqu'à c_S (ligne tiretée verticale), le modèle prédit (correctement) que $g^{(2)}(0)$ s'approche de 1.

d'une source de photons annoncés pour n'importe quelle valeur de la probabilité d'annonce. En guise de comparaison, une mesure directe de $g^{(2)}(0)$ à une probabilité d'annonce donnée nécessite la comptabilisation de plusieurs coups triples émanent de l'émission simultanée de plusieurs paires, lesquels sont beaucoup moins probables. Dans la présente expérience, à une probabilité d'annonce $P_S = 0{,}287\%$, la probabilité d'un coup double est environ 700 fois plus importante que la probabilité d'un coup triple. Ainsi, une mesure directe de $g^{(2)}(0)$ était beaucoup plus longue.

Notre méthode permet d'ajuster la luminosité très rapidement et sur demande. Elle sera donc très utile pour optimiser la performance de la DQC basée sur l'intrication, pour déterminer le niveau de sécurité de la DQC basée sur une source de photons annoncés et pour optimiser le taux d'erreur et la distance d'un répéteur quantique dans un contexte où les conditions expérimentales telles que la transmittance d'un canal fluctuent dans le temps.

3.6 Corrélations spectrales et spatiales

Le modèle que nous avons développé doit être modifié lorsque des corrélations spectrales et/ou spatiales existent entre les photons de chaque paire et que les transmittances des

canaux dépendent de la longueur d'onde et/ou du mode spatial des photons. Les corrélations spectrales émergent généralement lorsque la pompe est quasi monochromatique et que, par conséquent, sa largeur spectrale $\Delta\nu_p$ est très étroite. Dans ce cas, la largeur spectrale des photons est dictée uniquement par les propriétés du milieu non-linéaire et on a typiquement $\Delta\nu_s = \Delta\nu_c \gg \Delta\nu_p$. Malgré l'incertitude sur l'énergie de chaque photon, la connaissance de l'énergie de l'un détermine celle de l'autre. Autrement dit, les photons sont intriqués en fréquence et l'état global de la paire peut s'écrire comme

$$|\psi\rangle = \int_{-\infty}^{\infty} \mathrm{d}\Omega\, g(\Omega)|\nu_s - \Omega\rangle_s|\nu_c + \Omega\rangle_c, \tag{3.40}$$

où ν_s est la fréquence centrale du photon signal et $\nu_c = \nu_p - \nu_s$ est celle du photon complémentaire. La fonction $g(\Omega)$ est définie par les propriétés du milieu non-linéaire. Si le spectre du photon signal est rétréci par un filtre, le spectre du photon complémentaire est affecté de façon non-locale de sorte que les spectres modifiés respectent la condition de conservation de l'énergie [144]. Cette situation est typique dans l'implémentation d'une mesure dans la base de Bell car le spectre des deux photons à mesurer doit être filtré pour éliminer les corrélations spectrales [8]. Si on filtre également le photon complémentaire mais que le filtre utilisé ne correspond pas exactement au spectre modifié, la probabilité d'un coup double est réduite. Dans ce cas, les transmittances peuvent encore s'écrire comme η_S et η_A mais leur valeur est réduite en raison du filtrage. Lorsqu'une seule paire est émise, la probabilité de coup double est maintenant égale à $c\eta_S\eta_A$ (et non plus $\eta_S\eta_A$), où $0 \leq c \leq 1$ caractérise le désaccord des filtres. Une valeur $c = 1$ est atteinte soit lorsque les spectres des photons émis sont non corrélés avant le filtrage (une méthode pour réaliser ceci est démontrée dans la référence [145]), ou lorsque les spectres sélectionnés par les filtres satisfont la condition de conservation de l'énergie des photons. Dans ce cas, il n'est pas nécessaire de modifier notre modèle.

Les corrélations spatiales surviennent lorsque le vecteur d'onde de la pompe est très bien défini mais pas celui des photons de la paire. Leur incidence est la même que pour les corrélations spectrales : la probabilité d'un coup double est réduite à $c\eta_S\eta_A$. Globalement, la valeur de c tient compte à la fois des corrélations spectrales et des corrélations spatiales.

Lorsque $c < 1$, on peut montrer que la matrice M_η doit être modifiée ainsi :

$$M'_\eta = \begin{pmatrix}
1-\eta_S+(\eta_A+\eta_B)(c\eta_S-1) & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\eta_A(1-c\eta_S) & 1-\eta_B+\eta_S(c\eta_B-1) & 0 & 0 & 0 & 0 & 0 & 0 \\
\eta_B(1-c\eta_S) & 0 & 1-\eta_A+\eta_S(c\eta_A-1) & 0 & 0 & 0 & 0 & 0 \\
\eta_S(1-c(\eta_A+\eta_B)) & 0 & 0 & 1-(\eta_A+\eta_B) & 0 & 0 & 0 & 0 \\
0 & \eta_B(1-c\eta_S) & \eta_A(1-c\eta_S) & 0 & 1-\eta_S & 0 & 0 & 0 \\
c\eta_A\eta_S & \eta_S(1-c\eta_B) & 0 & \eta_A & 0 & 1-\eta_B & 0 & 0 \\
c\eta_B\eta_S & 0 & \eta_S(1-c\eta_A) & \eta_B & 0 & 0 & 1-\eta_A & 0 \\
0 & c\eta_B\eta_S & c\eta_A\eta_S & 0 & \eta_S & \eta_B & \eta_A & 1
\end{pmatrix}.$$

La présence de corrélations spectrales et/ou spatiales affecte les prédictions de notre modèle mais les conséquences sont minimes. Premièrement, pour une luminosité donnée, une valeur de c comprise dans l'intervalle $]0,1[$ a pour effet de rapprocher la valeur de G vers 1. Par exemple, la ligne continue de la fig. 3.5 correspond à $c = 1$, et la ligne tiretée à $c = 0{,}5$. Ainsi, on peut utiliser $c = 1$ sans affecter la validité de la borne supérieure de μ et de la borne inférieure de r obtenues en mesurant G. De plus, on peut montrer que les équations 3.35, 3.36 et 3.37 permettant de calculer les transmittances et la luminosité donneront les solutions suivantes lorsque les coups sombres sont négligés : $\eta'_S = c\eta_S$, $\eta'_A = c\eta_A$, $\eta'_B = c\eta_B$ et $\mu' = \mu/c$. Si ces mesures sont faites par un expérimentateur croyant à tort que $c = 1$, la conséquence directe est que les transmittances seront sous-estimées par un facteur c et la luminosité sera surestimée par un facteur $1/c$. Par contre, il est possible de montrer que ces effets s'annulent dans le calcul de $\mathbf{P}$ et, par conséquent, dans le calcul de $g^{(2)}(0)$. Pour ces raisons, il est possible que nous ayons légèrement surestimé la valeur de la luminosité, mais avons quand même prédit la bonne valeur de $g^{(2)}(0)$.

La sécurité de la DQC basée sur une une source de photons annoncés repose sur la connaissance de la valeur de μ. Si un expérimentateur utilise la méthode proposée ici pour mesurer μ en supposant que $c = 1$ et que, en réalité, ce n'est pas le cas, alors la luminosité sera surestimée, ce qui se traduira par une surestimation de l'information réellement disponible pour l'espion et par une réduction excessive du taux de génération de la clé par rapport à ce qui aurait été possible si $c = 1$ [47, 48]. Autrement dit, la sécurité de la DQC n'est pas affectée.

3.7 Conclusion

Nous avons développé un modèle décrivant de façon exacte la statistique des coups d'une source de paires de photons probabiliste. À l'aide de ce modèle, nous avons développé une méthode permettant d'estimer précisément les transmittances des canaux de transmission des photons émis et d'estimer la luminosité de la source à partir de la mesure des coups simples et doubles. Nous avons ensuite confirmé la validité de notre méthode en montrant qu'elle permet de prédire correctement la valeur de l'autocorrélation de second ordre $g^{(2)}(0)$ d'une source de photons annoncés. Cette méthode pourra donc être utilisée pour ajuster la luminosité sur demande et en temps réel dans le but d'optimiser les performances de la DQC basée sur l'intrication, de déterminer la sécurité de la DQC basée sur une source de photons annoncés et d'optimiser les performances d'un répéteur quantique. Finalement, nous avons montré que notre modèle permet de prédire correctement la statistique des coups même en présence de corrélations spectrales et/ou spatiales entre les photons émis, et que dans le pire

des cas, cela ne mène qu'à une surestimation de la luminosité de la source. Nous croyons que la simplicité de la méthode proposée la rendra très utile pour la communication quantique.

Les méthodes présentées ici ont aussi été utilisées pour caractériser une source de paires de photons basée sur un fibre optique microstructurée. Ces travaux ont été soumis pour publication et sont aussi disponibles sur l'archive web `arxiv.org` [146].

Chapitre 4

Intrication temporelle et non-localité

La source de paires de photons présentée au chapitre 3 a été utilisée pour construire une source d'intrication temporelle. Pour caractériser cette source, nous avons utilisé les idées développées au chapitre 2 et construit deux analyseurs temporels universels (ATU) qui, pour la première fois, permettent de mesurer chaque qubits temporels d'une paire intriquée dans une base arbitraire. La présence de l'intrication a été révélée par la mesure de la visibilité de l'intrication. [1] Cette mesure a été répétée plusieurs fois en utilisant différentes bases qui, lorsqu'elles sont disposées sur la sphère de Bloch, couvrent toutes les dimensions de cette dernière, mettant ainsi en évidence le caractère universel des ATU. Nous avons ensuite révélé la nature non-locale de notre source d'intrication temporelle avec un test de l'inégalité de Bell-CHSH. Grâce aux ATU, ce test a pu être répété plusieurs fois de sorte que, de test en test, le grand cercle de la sphère de Bloch contenant les bases de mesures utilisées pour un test donné était soumis à une rotation. L'ensemble des grands cercles utilisés couvre toutes les dimensions de la sphère de Bloch. Ces expériences ont d'abord été réalisées dans l'environnement contrôlé d'un laboratoire puis transportées *sur le terrain* où un des qubits de chaque paire était transmis par une fibre souterraine de 12,4 km installée entre l'Université de Calgary (UdeC) et le Southern Alberta Institute of Technology (SAIT).

La section 4.1 introduit la notion d'intrication et la section 4.2 présente le lien entre intrication et non-localité. Les sections 4.3 à 4.6 présentent une étude expérimentale de la non-localité d'une source d'intrication temporelle caractérisée avec des analyseurs temporels universels (ATU).

4.1 Intrication

4.1.1 Définition

Le principe de superposition est au cœur de la mécanique quantique (MQ). Si un système peut physiquement se trouver dans un état $|0\rangle$ ou dans l'état orthogonal $|1\rangle$, alors toute combinaison linéaire normée $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, où $|\alpha|^2 + |\beta|^2 = 1$, représente également un

1. La visibilité de l'intrication est définie à la section 4.2.1.

état physiquement réalisable. Lorsque le système étudié est composé de deux qubits, les états conjoints $|i\rangle \otimes |j\rangle \equiv |ij\rangle$, où $i, j \in \{0, 1\}$, forment une base orthonormée. Le principe de superposition indique alors que l'état

$$|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle, \tag{4.1}$$

où $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$, est physiquement réalisable. Étrangement, lorsque $\alpha\delta \neq \beta\gamma$, on peut montrer sans trop de difficultés qu'il est impossible de factoriser $|\Psi\rangle$ comme un produit tensoriel de deux états séparés :

$$|\Psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle, \tag{4.2}$$

où $|\psi_k\rangle = \alpha_k|0\rangle + \beta_k|1\rangle$ serait l'état du $k^{\text{ème}}$ qubit ($k = 1, 2$). Un tel état non factorisable (aussi appelé non séparable) est par définition un état intriqué. Formellement, cela signifie que la description du système conjoint ne peut s'exprimer comme l'ensemble des descriptions de chacune de ses parties.

Le caractère à la fois étrange et important de l'intrication devient évident lorsqu'on applique le postulat de la mesure à un système composé de deux qubits préparés dans un état intriqué.[2] Par exemple, lorsque le premier qubit d'une paire préparée dans l'état $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ est mesuré dans la base $\mathcal{B}_+ = \{|0\rangle, |1\rangle\}$, le résultat est aléatoire. Si ce résultat est $|i\rangle$, où $i \in \{0, 1\}$, l'état conjoint après la mesure est $(|i\rangle\langle i| \otimes \hat{I})|\Phi^+\rangle \propto |ii\rangle$, où $\hat{I}$ est l'opérateur identité. Par conséquent, le concept de l'*effondrement du paquet d'onde* nous dit que la mesure de ce deuxième qubit dans la base $\mathcal{B}_+$ donnera le même résultat que le premier, indépendamment de la distance entre les deux qubits. La signification physique de cet effondrement est un sujet de recherche en soi et une courte discussion est présentée à la section 4.2. Il suffit pour l'instant de noter que les corrélations parfaites entre les mesures faites sur chacun des qubits ne permettent pas de communiquer de l'information. En effet, lorsque le premier observateur mesure son qubit, le résultat de la mesure est complètement aléatoire, tout comme l'état du deuxième qubit.

Mathématiquement, l'état conjoint de deux qubits peut être exprimé comme une combinaison linéaire de quatre états intriqués formant une base orthonormée :

$$|\Psi\rangle = \alpha'|\Phi^+\rangle + \beta'|\Phi^-\rangle + \gamma'|\Psi^+\rangle + \delta'|\Psi^+\rangle, \tag{4.3}$$

2. Cette discussion est présentée dans le langage de l'information quantique, mais elle se transpose évidemment à tout système physique composé de deux (ou plusieurs) particules dont l'espace de Hilbert des états possibles est de dimension supérieure à deux, voir infinie.

où les états

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{4.4}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{4.5}$$

sont appelés *états de Bell* et correspondent aux états à deux qubits ayant un niveau d'intrication maximal.

L'intrication peut exister entre deux systèmes physiques distincts et séparés dans l'espace tels que deux photons (cf. section 4.1.2). Par exemple, deux photons peuvent être intriqués temporellement dans l'état $\frac{1}{\sqrt{2}}(|t_0, t_0\rangle + |t_1, t_1\rangle)$ ou en polarisation dans l'état $\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$.

L'intrication peut aussi exister entre deux degrés de liberté distincts du même système (comme un photon unique). Par exemple, considérons les bases $\{|H\rangle, |V\rangle\}$ et $\{|t_0\rangle, |t_1\rangle\}$ avec lesquelles l'état de polarisation et l'état temporel d'un qubit photonique peuvent s'exprimer. Un qubit temporel dans l'état $\frac{1}{\sqrt{2}}(|t_0\rangle + |t_1\rangle)$, dont la polarisation de la composante $|t_0\rangle$ est horizontale et celle de la composante $|t_1\rangle$ est verticale, se trouve en fait dans l'état

$$\frac{1}{\sqrt{2}}(|t_0, H\rangle + |t_1, V\rangle) \tag{4.6}$$

et est équivalent à l'état $|\Phi^+\rangle$. Il s'agit donc d'un état intriqué. Cette astuce a été utilisée pour augmenter le nombre de qubits par photon et faciliter la démonstration expérimentale de tâches telles que la téléportation quantique [60, 62] et le calcul quantique basé sur la mesure [82, 83, 84].

Un autre exemple d'intrication à un photon survient lorsqu'un photon unique est incident sur une séparatrice 50/50. En nommant a et b les modes de sortie de la séparatrice, l'état après la séparatrice peut s'exprimer dans la base de Fock :

$$\frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b + |1\rangle_a|0\rangle_b), \tag{4.7}$$

où $|1\rangle_a$ correspond à 1 photon dans le mode a, etc.

4.1.2 Intrication en polarisation, temporelle et hybride

Intrication en polarisation

Le développement des sources de paires de photons basées sur la conversion paramétrique spontanée (CPS) a ouvert la voie au développement de sources d'intrication de grande qualité.

Or, la CPS seule n'est pas suffisante pour obtenir de l'intrication en polarisation ou temporelle : il faut de plus que la paire de photon soit en superposition quantique d'avoir été créée par deux processus de CPS distincts. Ceci est mis en évidence dans la source d'intrication en polarisation développée en 1999 par P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum et P. H. Eberhard [20]. Deux cristaux biréfringents de BBO (borate de barium, BaB_2O_4) identiques sont placés en série et le deuxième est tourné de 90° autour de l'axe optique par rapport au premier (cf. fig. 4.1). L'accord de phase est de type I et, par conséquent, le premier cristal nécessite une pompe verticale pour produire une paire dans l'état $|HH\rangle$, et le deuxième nécessite une pompe horizontale pour produire une paire dans l'état $|VV\rangle$. En polarisant la pompe à 45°, chaque photon de la pompe est en superposition quantique de pomper le premier et le deuxième cristal de sorte que toute paire émergente est en superposition d'avoir été créée dans le premier et le deuxième cristal, avec la même probabilité. L'état de la paire est donc

$$\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle). \tag{4.8}$$

Une condition est essentielle pour obtenir un état intriqué avec cette source : les modes spatiaux, spectraux et longitudinaux des paires créées par un cristal ou l'autre doivent être identiques. Autrement dit, il doit être physiquement impossible de déterminer lequel des cristaux aurait créé la paire en mesurant un degré de liberté autre que la polarisation.

Au cours des quinze dernières années, l'intrication en polarisation a été abondamment utilisée [8] et il serait trop long de dresser un portrait complet de la situation. Il est cependant intéressant de mentionner que des photons intriqués en polarisation ont été générés dans plusieurs milieux non-linéaires avec différents types d'accord de phase comme les cristaux biréfringents avec un accord de phase de type II (ne nécessitant qu'un seul cristal au lieu de deux pour obtenir des photons intriqués) [19] et les cristaux « polés » périodiquement [147]. Le mélange à quatre ondes (M4O) spontané permet également de créer une source d'intrication en polarisation tel que démontré avec de la fibre optique à dispersion décalée [148] ainsi

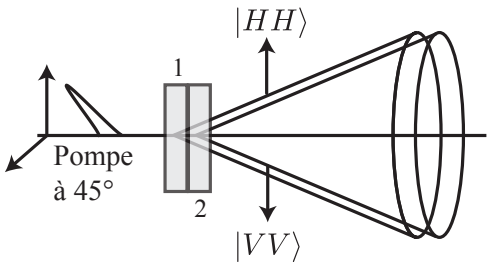

FIGURE 4.1 Source de qubits photoniques intriqués en polarisation.

qu'avec une fibre microstructurée [149].

Intrication temporelle

En 1999, J. Brendel, N. Gisin, W. Tittel et H. Zbinden ont développé une source d'intrication temporelle [3] exploitant le temps de création d'une paire comme degré de liberté pour coder les qubits [18]. L'idée consiste à pomper un cristal avec une impulsion de pompe où chaque photon de la pompe est préparé en une superposition temporelle $\frac{1}{\sqrt{2}}(|t_0\rangle + \mathrm{e}^{i\varphi}|t_1\rangle)$ (cf. section 2.1.2) à l'aide d'un interféromètre Mach-Zehnder à délai Δt (fig. 4.2). Lorsqu'une

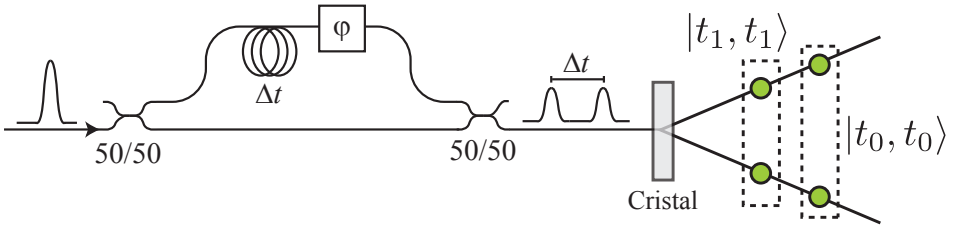

FIGURE 4.2 Source de qubits photoniques intriqués temporellement. L'impulsion de pompe, d'une durée τ, est incidente sur un interféromètre Mach-Zehnder à délai $\Delta t = t_1 - t_0 \gg \tau$. Chaque impulsion est donc préparée dans une superposition temporelle $\frac{1}{\sqrt{2}}(|t_0\rangle + \mathrm{e}^{i\varphi}|t_1\rangle)$ et pompe le milieu non-linéaire (ici représenté par un cristal). Les qubits générés par conversion paramétrique spontanée sont alors intriqués temporellement.

paire est créée par conversion paramétrique spontanée, elle est en superposition d'avoir été créée par la composante t_0 de la pompe, auquel cas la paire est dans l'état $|t_0, t_0\rangle$, et d'avoir été créée par la composante t_1, auquel cas la paire est dans l'état $\mathrm{e}^{i\varphi}|t_1, t_1\rangle$. Ainsi, l'état final de la paire est

$$\frac{1}{\sqrt{2}}(|t_0, t_0\rangle + \mathrm{e}^{i\varphi}|t_1, t_1\rangle). \tag{4.9}$$

La phase φ correspond à la phase relative entre les compostantes temporelles de la pompe. On peut s'en affranchir en définissant $|t_1'\rangle = \mathrm{e}^{i\varphi/2}|t_1\rangle$, ce qui correspond à décaler l'origine de t_1. Comme pour l'encodage temporel, on peut formellement définir l'intrication temporelle à l'aide d'un paquet d'ondes gaussien décrit par l'opérateur

$$\hat{T}^\dagger_{\omega_0}(t) = \int_{-\infty}^{\infty} \mathrm{d}\omega\, g(\omega - \omega_0)\mathrm{e}^{i\omega t}\hat{a}^\dagger_\omega\,. \tag{4.10}$$

3. « Time-bin entanglement ».

Cet opérateur crée un état temporel au temps t et de fréquence centrale ω_0 : $\hat{T}^\dagger_{\omega_0}(t)|0\rangle = |t\rangle_{\omega_0}$. Ainsi, l'état de deux qubits aux fréquences centrales ω_a et ω_b intriqués dans l'état $|\Phi^+\rangle$ est

$$\frac{1}{\sqrt{2}}\left(\hat{T}^\dagger_{\omega_a}(t_0)\hat{T}^\dagger_{\omega_b}(t_0) + \hat{T}^\dagger_{\omega_a}(t_1)\hat{T}^\dagger_{\omega_b}(t_1)\right)|0\rangle\,. \tag{4.11}$$

L'intrication temporelle été générée à partir de cristaux non-linéaires [18], dans une fibre optique à dispersion décalée [97] et dans un cristal « polé » périodiquement [150] (et cette thèse).

Intrication hybride

L'intrication est un concept indépendant de la réalisation physique qu'elle prend. Ainsi, deux systèmes différents peuvent êtres intriqués, tels le spin d'un atome et la polarisation d'un photon [151]. Lorsque les deux qubits sont photoniques, il devrait donc être possible d'intriquer la polarisation de l'un avec, par exemple, le mode spatial de l'autre. Ce type d'intrication *hybride*, proposée en 1991 par M. Żukowski et A. Zeilinger, n'a été démontrée pour la première fois que tout récemment [152, 153]. Cette source est intéressante pour le calcul quantique basé sur la mesure où plusieurs degrés de liberté d'un même photon sont exploités [82, 83, 84]. Elle semble être cependant d'intérêt limité pour la communication quantique car la transmission d'un qubit spatial sur une grande distance est extrêmement difficile à réaliser.

En 2007, nous avons proposé l'idée d'intriquer un qubit en polarisation avec un qubit temporel [154]. Ce type d'intrication hybride est décrit par un état du genre

$$\frac{1}{\sqrt{2}}(|H\rangle_1|t_0\rangle_2 + |V\rangle_1|t_1\rangle_2) \tag{4.12}$$

où $|H\rangle_1|t_0\rangle_2$ indique que le premier qubit photonique est dans l'état de polarisation $|H\rangle$ et le deuxième dans temporel $|t_0\rangle$, etc. Contrairement à l'état de l'éq. 4.6, les deux qubits sont encodés sur deux photons. Dans ce chapitre, nous présentons la première démonstration d'une telle source où un qubit de polarisation à 812 nm est intriqué avec qubit temporel à 1532 nm.

Interface quantique

Une source d'intrication hybride pourrait être utilisée en tant qu'interface quantique entre différents types de liens de transmission et différents types d'encodages. Cette interface pourrait être réalisée sans ou avec téléportation quantique, ainsi que nous le décrivons ici.

La grande différence entre les longueurs d'ondes de notre source d'intrication temporelle pourrait être utilisée pour créer une interface entre différents types de liens de transmission.

En effet, la transmission d'un qubit de polarisation à 812 nm est compatible avec un lien à l'air libre (biréfringence négligeable, atténuation minimale) et celle d'un qubit temporel à 1532 nm est compatible avec la fibre optique standard (atténuation minimale, faible coût). Les qubits distribués peuvent être mesurés directement pour réaliser une tâche comme la distribution quantique de clés. On peut aussi concevoir que le qubit de polarisation à l'air libre est transmis entre une station terrestre et un satellite en orbite autour de la terre tandis que le qubit temporel est transmis dans un réseau de fibre optique, tel qu'illustré à la fig. 4.3 [155]. Si le satellite est ré-orienté vers une autre station terrestre, cela permettrait à deux utilisateurs situés sur la Terre de communiquer en toute confidentialité, en supposant que le satellite est honnête. La contrainte d'un satellite honnête peut être éliminée s'il constitue une maillon d'un répéteur quantique (cf. section 1.5).

Cette source d'intrication hybride pourrait également être utilisée comme une interface permettant de téléporter l'état d'un qubit de polarisation à 812 nm sur un qubit temporel à 1532 nm. Plus précisément, considérons la fig. 4.4 correspondant à un montage de téléportation quantique. Le montage a pour but de téléporter l'état $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ du qubit de polarisation à 812 nm en utilisant une source d'intrication hybride créant l'état $\frac{1}{\sqrt{2}}(|H\rangle_1|t_0\rangle_2 + |V\rangle_1|t_1\rangle_2)$. Lorsque la mesure de Bell réussit et que la correction est appliquée, le qubit temporel est préparé dans l'état $|\psi\rangle = \alpha|t_0\rangle + \beta|t_1\rangle$. Ce type d'interface pourrait être très utile dans un réseau quantique composé de différents types de liens (air libre et fibre optique) et utilisant différents types d'encodages.

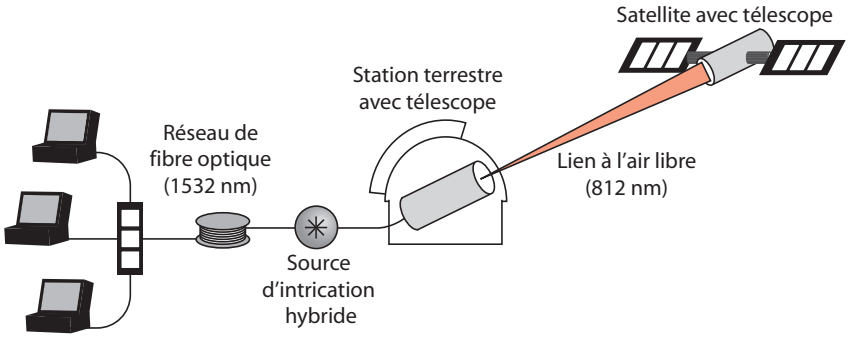

FIGURE 4.3 L'intrication hybride entre un qubit en polarisation à 812 nm et un qubit temporel à 1532 nm permet, en principe, de créer une interface quantique entre un réseau de fibre optique et lien à l'air à l'air libre.

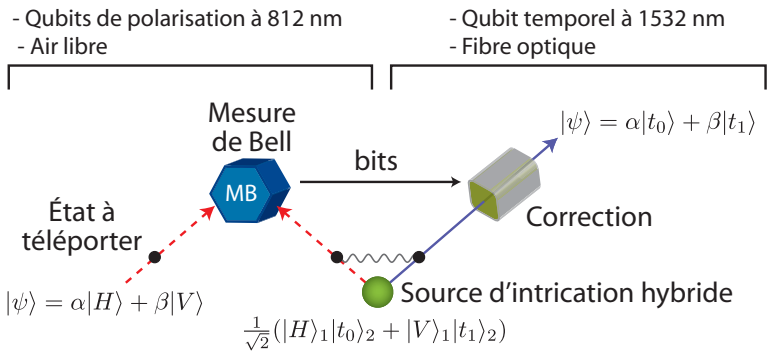

FIGURE 4.4 Interface quantique permettant de téléporter l'état d'un qubit de polarisation à 812 nm sur un qubit temporel à 1532 nm avec l'aide d'une source d'intrication hybride.

4.2 Intrication et non-localité

4.2.1 Théorème de Bell

L'intrication permet de créer des corrélations entre les résultats des mesures faites sur deux (ou plusieurs) systèmes physiques distincts. Par exemple, la mécanique quantique prédit que deux observateurs mesurant leur moitié respective de l'état $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ dans la base $\mathcal{B}_+ = \{|0\rangle, |1\rangle\}$ observeront le même résultat avec certitude, indépendamment de la distance qui les sépare et de qui mesure en premier. Ceci peut sembler en contradiction avec la relativité restreinte si on suppose que l'effondrement du paquet d'onde constitue une influence physique réelle et instantanée entre les deux qubits. En réalité, ce n'est pas le cas car l'intrication ne peut être utilisée pour transmettre de l'information plus rapidement que la vitesse de la lumière.

La mécanique quantique n'explique pas l'origine des corrélations issues de l'intrication, elle ne fait que donner la recette permettant de les prédire. En 1935, A. Einstein, B. Podolsky et N. Rosen (EPR), alors insatisfaits de cette situation, ont émis l'hypothèse que la MQ est une description incomplète de la réalité. Selon EPR, la MQ doit être complétée par l'ajout de *variables locales cachées* lui redonnant un caractère plus « réaliste ». Ces variables locales cachées peuvent être vues comme des propriétés physiques potentiellement inaccessibles, inconnues et propres à chaque qubit d'un paire donnée. Elles sont initialisées au moment de la création de la paire et déterminent (ou influencent) le résultat de la mesure faite sur le qubit auquel elles sont rattachées. La ou les variables cachées associées à un qubit donné peuvent évoluer au cours de la transmission, mais cette évolution ne peut être influencée que par des événements situés dans le cône de lumière du qubit en question. Ceci est l'hypothèse de la *localité*.

Pendant une trentaine d'années, le débat initié par EPR fut philosophique. Puis, en 1964, il prit une tournure importante lorsque J. S. Bell découvrit qu'une théorie à variables locales cachées, que nous nommerons désormais *théorie locale*, est incapable de reproduire toutes les prédictions de la mécanique quantique [22, 156] ; ceci constitue le *théorème de Bell*. Ce théorème peut, en principe, être testé expérimentalement, ce qui recentra le débat sur l'arène de la physique. Le test proposé à l'origine par Bell a été modifié par J. F. Clauser, M. A. Horne, A. Shimony et R. A. Holt (CHSH) pour tenir compte de certaines limitations expérimentales, ce qui a nécessité l'ajout d'hypothèses [24]. Ce test est décrit dans les paragraphes qui suivent.

Soit deux observateurs, Alice et Bob, recevant chacun un qubit d'une paire intriquée dans l'état $|\Phi^+\rangle$ provenant d'une source située quelque part entre leur positions respectives (fig. 4.5). [4] Alice (Bob) fait ensuite le choix de mesurer son qubit dans la base A_1 (B_1) avec une probabilité 1/2 ou dans la base A_2 (B_2) avec une probabilité 1/2. Le moment où Bob fait ce choix ne doit pas être situé dans le cône de lumière du choix d'Alice (et vice versa). Cette condition est nécessaire pour éliminer la possibilité que le choix d'Alice et le résultat de sa mesure ne puissent influencer le résultat de Bob (et vice versa), tel qu'expliqué dans la section 4.2.2. La mesure du qubit d'Alice produit le résultat $a \in \{+1, -1\}$ et la mesure du qubit de Bob produit $b \in \{+1, -1\}$. Lorsque les deux qubits sont détectés, les résultats possibles sont notés $++$, $+-$, $-+$ et $--$. Alice et Bob recommencent un grand nombre de fois et compilent les statistiques issues des coups doubles. [5] Soit N_{++}^{ij} le nombre de coups doubles observés durant une période de temps Δt donnée et ayant produit le résultat $++$ lorsqu'Alice a mesuré dans la base A_i et Bob dans la base B_j ($i, j \in \{1, 2\}$). On définit le coefficient de corrélation suivant :

$$E_{ij} = \frac{N_{++}^{ij} + N_{--}^{ij} - N_{+-}^{ij} - N_{-+}^{ij}}{N_{++}^{ij} + N_{--}^{ij} + N_{+-}^{ij} + N_{-+}^{ij}}. \tag{4.13}$$

Cette équation peut être ré-écrite comme

$$E_{ij} = P_{++}^{ij} + P_{--}^{ij} - P_{+-}^{ij} - P_{-+}^{ij}, \tag{4.14}$$

où $P_{++}^{ij} = N_{++}^{ij}/(N_{++}^{ij} + N_{--}^{ij} + N_{+-}^{ij} + N_{-+}^{ij})$ est la probabilité d'obtenir le résultat $++$ par coup double. Ce coefficient correspond à la valeur espérée du produit ab lorsqu'Alice et Bob

4. Le raisonnement pourrait être repris avec un des trois autres états de Bell est les conclusions seraient les mêmes.

5. Un coup double correspond à une détection chez Alice et une chez Bob

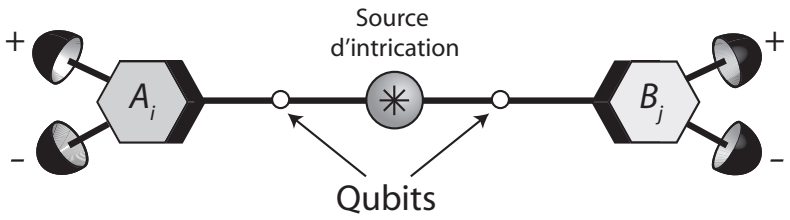

FIGURE 4.5 Configuration expérimentale permettant à deux observateurs, Alice et Bob, de tester le théorème de Bell. Pour chaque paire émise, Alice et Bob mesurent leur qubit respectif dans les bases A_i et B_j choisies aléatoirement. La détection d'un qubit produit le résultat $+1$ ou -1 et seuls les coups doubles entre Alice et Bob sont considérés.

mesurent dans les bases i et j respectivement :

$$E_{ij} = \sum_{a=-1}^{+1} \sum_{b=-1}^{+1} ab\, P(a,b|i,j), \tag{4.15}$$

où $P(a,b|i,j) \equiv P_{ab}^{ij}$.

Après avoir accumulé suffisamment d'événements, Alice et Bob sont en mesure d'assigner des valeurs à E_{11}, E_{12}, E_{21}, E_{22} et au paramètre S suivant :

$$S = |E_{11} - E_{12} + E_{21} + E_{22}|. \tag{4.16}$$

La valeur de ce paramètre servira de critère pour comparer les prédictions de la MQ et celle d'une théorie locale. Les bases A_1, A_2, B_1 et B_2 peuvent être arbitraires, mais la valeur de S en dépend. Il existe un choix de bases permettant d'optimiser la séparation entre les prédictions d'une théorie locale et celles de la MQ.

Commençons d'abord par les prédictions d'une théorie locale. Toute théorie de ce type est telle que l'on peut écrire la probabilité conjointe $P(a,b|i,j)$ comme

$$P(a,b|i,j) = \sum_{\lambda} p(\lambda) P(a|i,\lambda) P(b|j,\lambda), \tag{4.17}$$

où λ représente l'état des variables locales cachées d'Alice et Bob, $p(\lambda)$ est la probabilité que ces variables soient initialisées dans l'état λ et $P(a|i,\lambda)$ est la probabilité qu'Alice obtienne le résultat a en mesurant dans la base i pour une valeur λ donnée, etc. Il est maintenant clair que le résultat de la mesure d'Alice ne peut être influencé par celle de Bob car la probabilité conjointe est un mélange statistique de probabilités séparables. Nous n'en ferons

pas la preuve, mais il est possible de montrer qu'une théorie locale produit la borne suivante :

$$S \leq 2 \quad \text{(théorie locale)}. \tag{4.18}$$

Ceci est l'*inégalité de Bell-CHSH* [24].

Calculons maintenant la valeur de S prédite par la mécanique quantique. On tient compte de la possibilité que la source soit imparfaite en supposant qu'elle prépare l'état $|\Phi^+\rangle$ avec probabilité V et l'état $\rho = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$ avec probabilité $1-V$. L'état ρ correspond au mélange statistique de $|00\rangle$ et $|11\rangle$ et n'est pas intriqué. La description de l'état préparé par la source est donc

$$\rho' = V|\Phi^+\rangle\langle\Phi^+| + (1-V)\rho. \tag{4.19}$$

Supposons d'abord qu'Alice mesure dans la base

$$A_1 = \left\{ \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\} \equiv \{|+\rangle, |-\rangle\} \tag{4.20}$$

et que Bob mesure dans la base

$$B_1 = \left\{ \tfrac{1}{\sqrt{2}}(|0\rangle + \mathrm{e}^{i\varphi}|1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle - \mathrm{e}^{i\varphi}|1\rangle) \right\} \equiv \{|+\rangle_\varphi, |-\rangle_\varphi\}\,. \tag{4.21}$$

Soit η_A (η_B), la transmittance totale du canal d'Alice (Bob), incluant l'efficacité des détecteurs. Supposons que la source d'intrication soit produite à partir de la conversion paramétrique spontanée avec un laser de pompe pulsé et notons p_1 la probabilité de créer une paire par impulsion de pompe (on néglige la contribution des coups sombres et l'éventualité que la source génère plus d'une paire). La probabilité de détecter un coup double par impulsion de pompe est

$$\begin{aligned} \tilde{P}^{11}_{++} &= p_1\eta_A\eta_B\Big({}_\varphi\langle +|\langle +|\rho'|+\rangle|+\rangle_\varphi\Big) && (4.22)\\ &= \frac{p_1\eta_A\eta_B}{2}(1 + V\cos\varphi) && (4.23) \end{aligned}$$

On peut maintenant calculer la probabilité du résultat ++ par coup double :

$$\begin{aligned} P^{11}_{++} &= \frac{\tilde{P}^{11}_{++}}{\tilde{P}^{11}_{++} + \tilde{P}^{11}_{+-} + \tilde{P}^{11}_{-+} + \tilde{P}^{11}_{--}} && (4.24)\\ &= \frac{1}{4}(1 + V\cos\varphi). && (4.25) \end{aligned}$$

De la même façon on trouve que $P^{11}_{--} = P^{11}_{++}$ et que $P^{11}_{+-} = P^{11}_{-+} = (1 - V\cos\varphi)/4$. Le

coefficient de corrélation correspondant est

$$E_{11} = V \cos\varphi. \tag{4.26}$$

Après avoir refait le même calcul pour les coefficients E_{12}, E_{21} et E_{22}, il est possible de montrer [157] que la valeur de S peut être maximisée en choisissant $\varphi = \pi/4$ (ce qui fixe la base B_1) et les bases A_2 et B_2 suivantes :

$$A_2 = \left\{|+\rangle_{\frac{\pi}{2}}, |-\rangle_{\frac{\pi}{2}}\right\} \tag{4.27}$$

$$B_2 = \left\{|+\rangle_{\frac{3\pi}{4}}, |-\rangle_{\frac{3\pi}{4}}\right\}. \tag{4.28}$$

On peut représenter ces bases sur la sphère de Bloch (fig. 4.6). Elles sont distribuées de façon symétrique sur l'équateur. Cette configuration donne $E_{11} = -E_{12} = E_{21} = E_{22} = V/\sqrt{2}$ et donc $S = 2\sqrt{2}V$. Ainsi, on a l'inégalité suivante pour la valeur prédite par la mécanique quantique :

$$S \leq 2\sqrt{2} \approx 2{,}828. \tag{4.29}$$

La valeur maximale nécessite une source parfaite ($V = 1$). Il est possible de montrer que ceci est la plus grande valeur possible lorsqu'Alice et Bob reçoivent des qubits et utilisent deux bases de mesures chacun [157]. Expérimentalement, une mesure produisant $S > 2$ constitue une violation de l'inégalité de Bell-CHSH et montre que les corrélations entre les résultats des mesures faites sur l'état quantique partagé par Alice et Bob ne peuvent être expliquées par une théorie locale. Autrement dit, la mécanique quantique est une *théorie non-locale*. Les premières démonstrations de la violation d'une inégalité de Bell-CHSH ont été réalisées

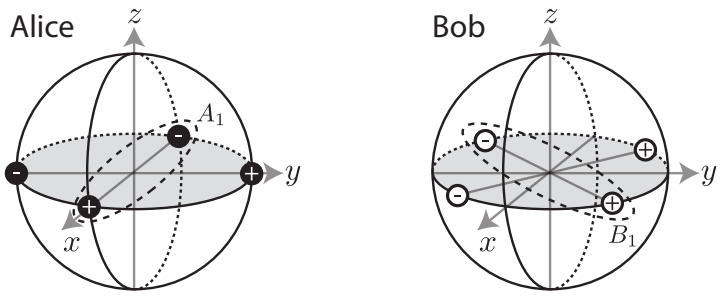

FIGURE 4.6 Bases de mesures de l'inégalité Bell-CHSH. Chaque base est définie par deux cercles pleins noirs (pour Alice) ou blancs (pour Bob) diamétralement opposés (les bases A_1 et B_1 sont indiquées). Le cercle contenant le signe « + » correspond au résultat +1 et celui contenant le signe « − » et correspond au résultat −1. Les bases A_1 et A_2 sont représentées sur la sphère de gauche et les bases B_1 et B_2 sur la sphère de droite.

au cours des années 70 et 80 [25, 26, 27, 28]. La référence [8] dresse un portrait historique des événements. Aujourd'hui, la mesure du paramètre S est souvent utilisé comme standard permettant quantifier la qualité d'une source d'intrication.

La configuration présentée à la fig. 4.6 n'est pas la seule permettant d'atteindre la borne $S = 2\sqrt{2}$. En effet, on obtient la même valeur si une transformation unitaire quelconque est appliquée à toutes les bases.[6] Autrement dit, la valeur de S est, en théorie, *invariante par rotation*. Une vérification expérimentale de cette prédiction est présentée à la section 4.5.3.

Visibilité de l'intrication

Par analogie avec la visibilité interférométrique, on nomme la quantité V *visibilité de l'intrication* car, en faisant varier la phase φ, la probabilité $\tilde{P}^{11}_{++}$ oscille sinusoïdalement et la visibilité de la courbe obtenue est

$$\begin{aligned} \text{Visibilité de } \tilde{P}^{11}_{++} &= \frac{\max - \min}{\max + \min} && (4.30)\\ &= \frac{(1+V)-(1-V)}{(1+V)+(1-V)} && (4.31)\\ &= V. && (4.32) \end{aligned}$$

Ce résultat tient également pour $\tilde{P}^{11}_{+-}$, $\tilde{P}^{11}_{-+}$ et $\tilde{P}^{11}_{--}$.

La mesure de la visibilité de l'intrication permet d'évaluer la qualité d'une source en fonction de plusieurs critères que nous énonçons ici. Premièrement, une visibilité supérieure à $\frac{1}{3} \approx 33{,}3\%$ implique que les qubits de la source sont bel et bien intriqués [158]. Deuxièmement, une visibilité supérieure à $1/\sqrt{2} \approx 70{,}7\%$ permet de prouver, moyennant deux hypothèses supplémentaires, que les corrélations ne peuvent être expliquées par une théorie locale [159, 160]. Troisièmement, il est possible de montrer que la distribution quantique de clés basée sur l'intrication est sécuritaire contre des attaques individuelles uniquement si $V > 1/\sqrt{2} \approx 70{,}7\%$ et contre des attaques cohérentes uniquement si $V > 78\%$ [161, 162, 9].

4.2.2 Échappatoires

La violation expérimentale d'une inégalité de Bell comporte toujours une certaine part d'imperfections. Dans certaines situations, celles-ci ouvrent la porte à l'élaboration de théories locales permettant de recréer les corrélations observées. Nous présentons ici les deux échappatoires[7] les plus importantes, soit celle de la localité et celle du rendement.

6. Cette transformation définit un nouveau grand cercle contenant toutes les bases de mesures.
7. « Loopholes ».

L'*échappatoire de la localité* a été envisagée par EPR dès 1935 et survient lorsque l'hypothèse de la localité n'est pas respectée (cf. section 4.2.1). Il est très simple de concevoir une théorie locale violant une inégalité de Bell lorsque les choix de bases d'Alice et Bob peuvent s'influencer de façon causale. À ce jour, deux expériences satisfaisant le critère de la localité ont été réalisées [29, 59].

Lorsque les transmittances des canaux d'Alice et Bob sont très faibles, il est à nouveau possible de concevoir une théorie locale violant l'inégalité de Bell-CHSH [163]. Ceci constitue l'*échappatoire du rendement.*[8] Le seuil de rendement sous lequel cela devient possible est $\eta_A = \eta_B \approx 82{,}8\%$ [164]. Ce seuil peut être réduit à environ 67% en utilisant des états au niveau d'intrication moindre qu'un état de Bell [165]. À ce jour, aucune expérience basée sur l'intrication photonique n'a réussi à dépasser ce seuil. Par conséquent, elles ont toutes eu recours à l'hypothèse d'*échantillonnage non biaisé*[9] des mesures. Cette échappatoire a été éliminée dans une expérience utilisant des ions intriqués. Dans cette expérience, le rendement était très près de 100% [166].

Aucune expérience n'a réussi à éliminer ces deux échappatoires simultanément.

4.2.3 Autres inégalités

À part l'inégalité de Bell-CHSH, il existe d'autres inégalités testant différents aspects de la non-localité. Les deux que nous présentons ici nécessitent la possibilité de mesurer les qubits d'une paire intriquée dans plusieurs bases qui ne peuvent toutes être disposées sur le même grand cercle et qui couvrent donc toutes les dimensions de la sphère de Bloch. Ceci est en contraste avec l'inégalité de Bell-CHSH qui nécessite uniquement la possibilité de mesurer dans des bases disposées sur un grand cercle de la sphère de Bloch.

Inégalité de Leggett

En 2003, A. J. Leggett a développé une théorie non-locale soumise à quelques contraintes permettant de la séparer de la MQ [34]. Le caractère non-local s'exprime dans le fait que la probabilité conjointe $P(a, b|i, j)$ n'est pas soumise à l'éq. 4.17. Cette contrainte est remplacée par la suivante : les probabilités marginales $P(a|i, \lambda)$ et $P(b|j, \lambda)$ doivent reproduire les statistiques équivalentes à la situation où Alice et Bob partagent un état séparable au lieu d'un état intriqué [167, 168]. A. J. Leggett a montré que les corrélations prédites par cette théorie permettent de violer l'inégalité de Bell-CHSH mais qu'elles ne peuvent reproduire toutes les prédictions de la mécanique quantique. Une expérience dont le résultat est borné par une

8. « Detection efficiency loophole »
9. « Fair sampling ».

inégalité (que l'on nomme *inégalité de Leggett*) a été proposée.

La violation expérimentale d'une inégalité de Leggett nécessite une source d'intrication dont la visibilité est très élevée ($\gtrsim 94{,}3\%$) et la possibilité de mesurer dans plusieurs bases couvrant toutes les dimensions de la sphère de Bloch. La première violation a été réalisée en 2007 à l'aide de l'intrication en polarisation [169]. Plusieurs améliorations ont ensuite été rapportées [167, 168, 35].

L'inégalité « élégante »

Une autre inégalité de Bell nécessitant la mesure dans plusieurs bases couvrant toutes les dimensions de la sphère de Bloch est l'inégalité « élégante », nommée ainsi par N. Gisin [170]. Une violation de cette inégalité permettrait de démontrer que l'espace de Hilbert des qubits émis par la source d'intrication doit nécessairement être complexe pour expliquer l'origine des corrélations [170]. Au meilleur de notre connaissance, aucune violation de cette inégalité n'a été réalisée.

4.3 Étude de la non-localité avec analyseurs temporels universels

Le reste de ce chapitre est consacré à l'étude expérimentale d'une source d'intrication temporelle. Pour réaliser cette étude, nous avons construit deux analyseurs temporels universels (ATU) suivant une proposition faite à la section 2.1.4. Ceci nous a permis d'accomplir pour la première fois les tâches suivantes :

- l'analyse des qubits d'une source d'intrication temporelle dans des bases arbitraires,
- la démonstration d'une source d'intrication hybride entre un qubit de polarisation et un qubit temporel,
- la vérification de l'invariance par rotation de l'inégalité de Bell-CHSH (telle que définie à la p. 77),
- l'implémentation d'un nouveau protocole de pile ou face quantique tolérant aux pertes (ceci est présenté au chapitre 5).

Pour chacune de ces tâches, un qubit de chaque paire était transmis d'abord sur une fibre optique de quelques mètres. Ensuite, ce court lien a été remplacé par un fibre optique souterraine de 12,4 km reliant l'université de Calgary (UdeC) au collège SAIT. À vol d'oiseau, les deux laboratoires sont séparés par 3,3 km.

4.4 Montage expérimental

Nous débutons par une description détaillée des deux ATU. On rappelle que l'ATU permet de mesurer un qubit temporel dans n'importe quelle base en le convertissant d'abord en un qubit de polarisation.

4.4.1 Analyseur temporel universel à l'air libre

Le premier ATU est conçu pour mesurer un qubit à 810 nm transmis à l'air libre et est schématisé à la fig. 4.7. Supposons que le qubit incident se trouve dans l'état $|\psi\rangle = \cos\theta|t_0\rangle + \mathrm{e}^{i\phi}\sin\theta|t_1\rangle$ et qu'il soit polarisé horizontalement. Sur la fig. 4.7, la composante $|t_0\rangle$ ($|t_1\rangle$) est représentée par la ligne continue (pointillée). À l'aide de la lame demi-onde D1, la polarisation du qubit est d'abord orientée à 45° par rapport à la polarisation rectiligne transmise par le cube polariseur C1. Ainsi, chaque composante est séparée également entre les deux bras de l'interféromètre composé de C1 et des rétro-réflecteurs R1 et R2. Les composants optiques de l'interféromètre sont collés sur une plaque de verre de type « Zerodur » (fabriquée par Schott) possédant un coefficient de dilatation thermique quasi nul. De plus, l'interféromètre est placé dans une boîte dont la température est maintenue à 28 °C grâce à un régulateur de

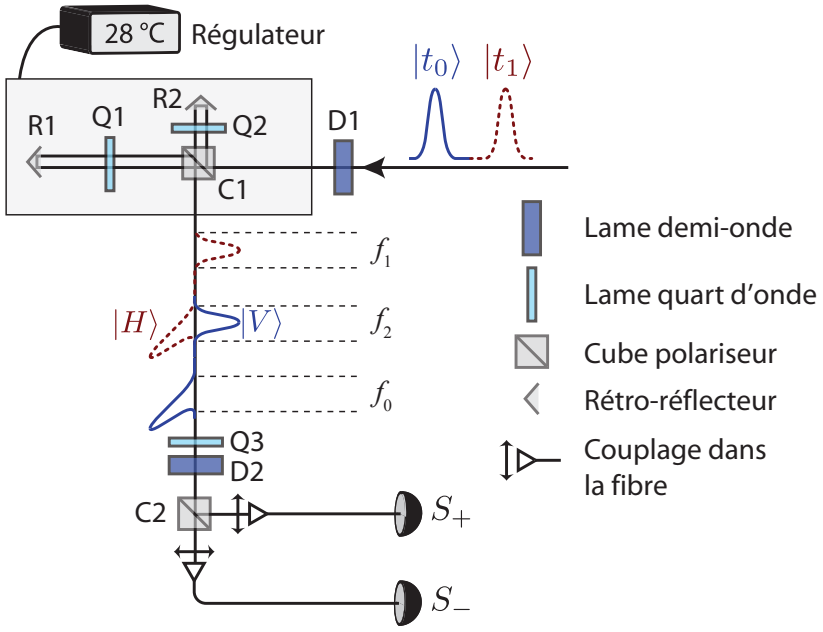

Figure 4.7 ATU conçu pour mesurer un qubit temporel à 810 nm transmis à l'air libre. Le qubit temporel incident est converti en un qubit de polarisation (dans la fenêtre temporelle f_2) et mesuré dans une base arbitraire sélectionnée par l'orientation des lames Q3 et D2.

température. Chaque faisceau incident sur R1 et R2 est réfléchi parallèlement à lui-même avec un léger décalage spatial. Le double passage dans les lames quart d'onde Q1 et Q2 permet de tourner la polarisation de chaque faisceau de 90° et le faisceau du bras court (long) est transmis (réfléchi) à C1 vers le bas. La différence de temps entre les bras est égale à $t_1 - t_0 = \Delta t = 1{,}4$ ns. À la sortie de l'interféromètre, les composantes du qubit initial ont chacune évolué en deux composantes supplémentaires aux polarisations orthogonales et décalées par Δt tel qu'illustré. Dans la fenêtre f_2, la composante $|t_0\rangle$ ($|t_1\rangle$) a évolué vers $|V\rangle$ ($|H\rangle$) et on a maintenant un qubit de polarisation dans l'état $|\psi'\rangle = \cos\theta|V\rangle + \mathrm{e}^{i(\phi+\phi_A)}\sin\theta|H\rangle$, où ϕ_A est une phase additionnelle causée par l'interféromètre. En choisissant l'orientation des lames de retard Q3 et D2, on peut mesurer ce qubit de polarisation dans une base arbitraire. Les sorties de C2 sont couplées dans une fibre optique unimodale à 810 nm. Les fibres sont ensuite dirigées vers les détecteurs de photon au silicium S_+ et S_-.

Chaque détection survient dans la fenêtre temporelle f_2 avec une probabilité de 50%. Autrement, elle survient dans f_0 avec une probabilité de 25% et dans f_1 avec une probabilité de 25%, ce qui correspond à une projection sur les états $|t_0\rangle$ ou $|t_1\rangle$, respectivement. Tous les résultats présentés dans ce chapitre sont tels que seuls les coups enregistrés dans la fenêtre f_2 étaient comptabilisés.

4.4.2 Analyseur temporel universel tout-fibre

Le deuxième ATU que nous avons fabriqué est conçu pour une longueur d'onde d'environ 1530 nm. Il est schématisé à la fig. 4.8. Le contrôleur de polarisation CP1 permet d'abord d'orienter la polarisation du qubit incident afin d'optimiser la transmission à travers le cube polariseur C3 (on suppose que l'état de ce dernier est $|\psi\rangle = \cos\theta|t_0\rangle + \mathrm{e}^{i\phi}\sin\theta|t_1\rangle$). À la sortie de C3, la polarisation du qubit temporel est rectiligne et est couplée dans l'axe lent d'une fibre optique à maintien de polarisation (représentée par un trait gras). L'axe lent de la fibre est ensuite tourné de 45° par rapport à la polarisation rectiligne transmise par le cube C4 de façon à ce que chaque composante du qubit temporel incident soit séparée également entre les deux sorties de C4. À ces sorties, la lumière est couplée dans l'axe lent de fibres à maintien de polarisation. Le bras court et le bras long sont combinés au cube C5. Dans la fenêtre f_2, l'état juste après C5 est donc $|\psi''\rangle = \cos\theta|V\rangle + \mathrm{e}^{i(\phi+\phi_B)}\sin\theta|H\rangle$. La phase ϕ_B peut être modulée grâce à un actuateur piézoélectrique PZ en forme de cylindre creux et autour duquel une section du bras long de l'interféromètre est enroulée. L'orientation des boucles du contrôleur de polarisation de Lefèvre [103], combinée avec le cube C6, permettent de sélectionner la base de mesure. Comme pour l'ATU à l'air libre, on ne considère que les cas où le qubit est détecté dans la fenêtre f_2, ce qui survient avec une probabilité de 50%. Les coups sont enregistrés par les détecteurs de photons InGaAs I_+ et I_-.

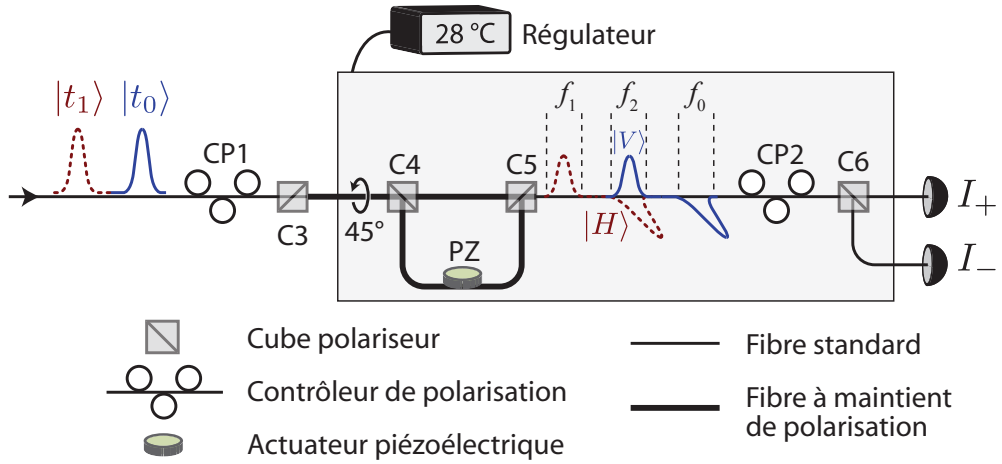

FIGURE 4.8 ATU tout-fibre conçu pour mesurer un qubit temporel à 1530 nm. Le qubit temporel incident est converti en un qubit de polarisation (dans la fenêtre temporelle f_2) et est mesuré dans une base arbitraire sélectionnée par l'orientation du contrôleur de polarisation CP2.

Les boucles de CP2 sont ajustées de la façon suivante. Tout d'abord, une impulsion lumineuse intense préparée dans l'état $|t_0\rangle$ est incidente sur l'ATU. Nous ne considérerons que la composante de $|t_0\rangle$ qui a parcouru le bras court. Juste après C5, cette composante est dans l'état $|H\rangle$ et dans la fenêtre f_0. Le contrôleur CP2 la transforme ensuite dans l'état $\cos\alpha|H\rangle + \mathrm{e}^{i\beta}\sin\alpha|V\rangle$. L'intensité de l'impulsion transmise par C6 est proportionnelle à $\cos^2\alpha$ et peut être mesurée en remplaçant I_+ par un détecteur linéaire rapide branché sur un oscilloscope. En ajustant l'orientation des boucles, on peut maximiser l'amplitude de l'impulsion observée, ce qui implique que $\alpha = 0$. On peut ensuite sélectionner la valeur de α désirée en ajustant les boucles pour obtenir une intensité réduite par un facteur $\cos^2\alpha$. La valeur de β ne peut être mesurée directement de cette façon : ceci nécessiterait une tomographie l'état de polarisation. Heureusement, ce n'était pas nécessaire pour accomplir nos objectifs (comme expliqué plus loin).

4.4.3 Source d'intrication temporelle

La source d'intrication temporelle que nous avons construite est schématisée sur la fig. 4.9. L'état créé est

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(|t_0\rangle_A|t_0\rangle_B + |t_1\rangle_A|t_1\rangle_B\big) \tag{4.33}$$

où $|t_i\rangle_A$ ($|t_i\rangle_B$) représente l'état temporel t_i d'Alice (Bob). Pour obtenir cet état, une diode laser crée des impulsions de 50 ps à 530,6 nm avec un taux de répétition de 20 MHz. Les

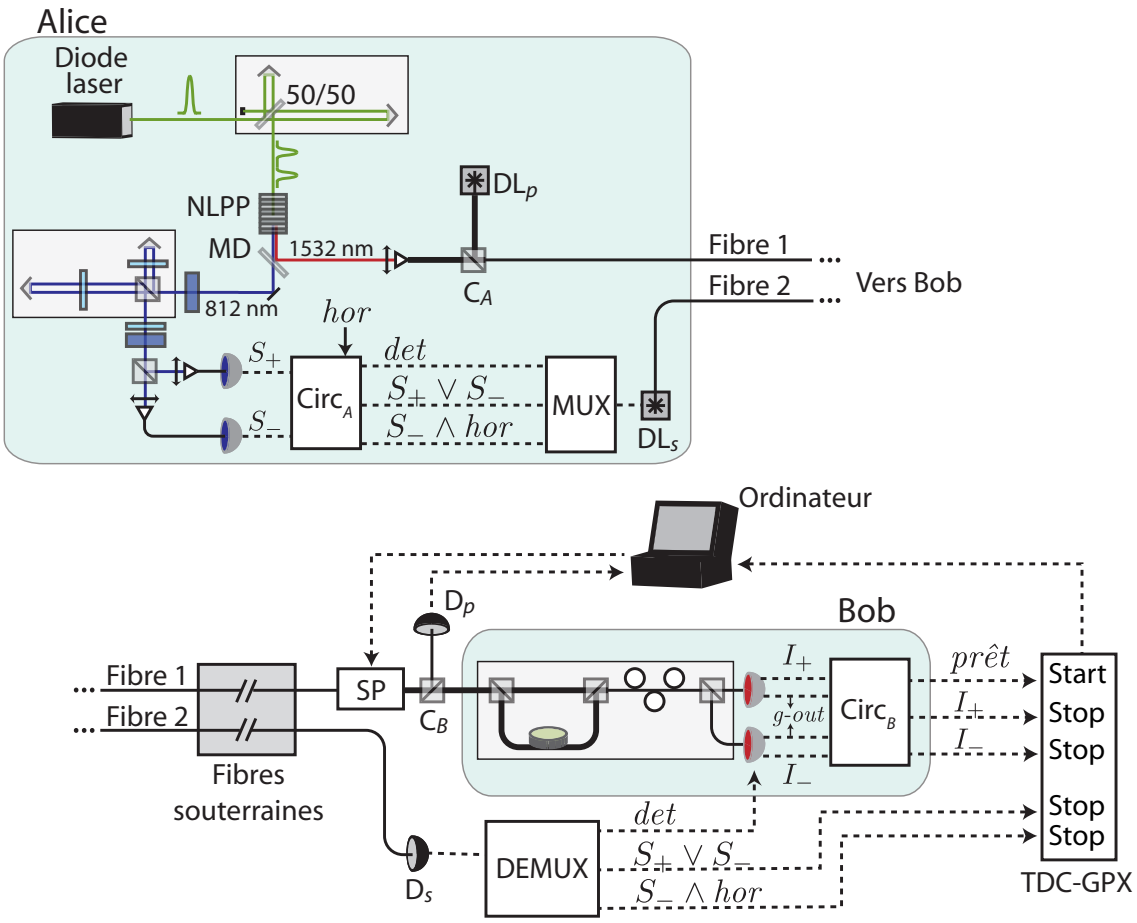

FIGURE 4.9 Source d'intrication temporelle.

impulsions sont incidentes sur un interféromètre Mach-Zehnder replié sur lui-même (ce qui est analogue à un interféromètre de Michelson) et ayant un délai de 1,4 ns. Tout comme pour l'ATU à l'air libre, les composants optiques de cet interféromètre sont collés sur une plaque de verre « Zerodur » et placés dans une boîte dont la température est régulée. À la sortie de cet interféromètre, chaque impulsion est préparée dans l'état temporel $\frac{1}{\sqrt{2}}(|t_0\rangle + |t_1\rangle)$. Chaque impulsion pompe le cristal NLPP dans lequel des paires de photons intriqués temporellement aux longueurs d'ondes centrées sur 811,7 et 1532,2 nm sont créées par conversion paramétrique spontanée. Le rapport $r = p_1/p_{n>1}$ (p. 53) de la probabilité de créer une paire sur celle de créer plus d'une paire était environ égal à 20 ce qui nous assure que l'émission simultanée de plus d'une paire ne contribuait pas significativement aux résultats. Les paires sont séparées par un miroir dichroïque MD et la pompe est éliminée par des filtres passe-haut. Le qubit à 811,7 nm est mesuré directement par Alice à l'aide de l'ATU à l'air libre. Le qubit à 1532,2 nm est, pour sa part, couplé dans la fibre pour être transmis vers Bob.

4.4.4 Transmission

Deux séries de mesures ont été réalisées. Dans la première, Bob était placé sur la même table optique qu'Alice. Dans la deuxième, Bob se trouvait à SAIT et les photons étaient transmis par le biais d'une fibre optique souterraine. La fig. 4.9 correspond à la configuration utilisée pour la deuxième série de mesures, que nous décrivons d'abord. Le lien souterrain est en fait composé de deux fibres optiques unimodales à 1550 nm. Chaque fibre est longue de 12,4 km (ceci a été mesuré à l'aide d'un réflectomètre optique dans le domaine temporel [10]) et comporte une perte de 7,3 dB, soit 0,59 dB/km. En guise de comparaison, une fibre SMF28 comporte une perte d'environ 0,25 dB/km. Par conséquent, 7,3 dB équivaut environ à un lien de 30 km de fibre SMF28. La fig. 4.10 montre une vue satellite d'une partie de la ville de Calgary où les emplacements d'Alice et de Bob sont indiqués.

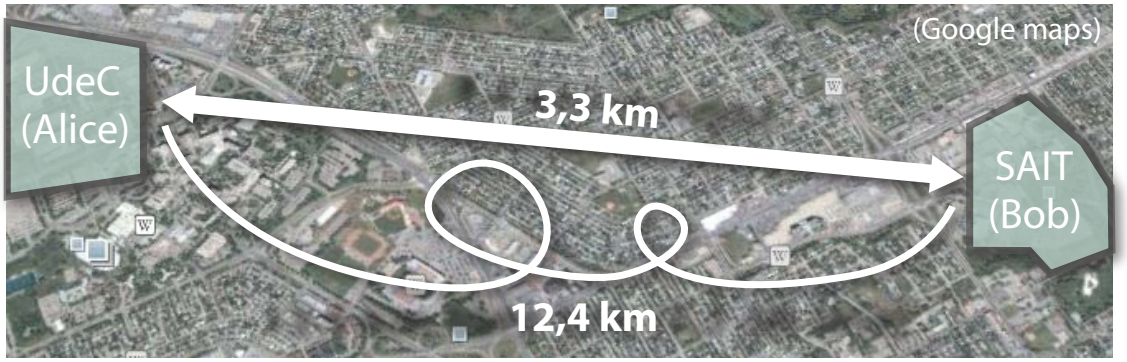

FIGURE 4.10 Vue aérienne de la ville de Calgary avec emplacements d'Alice et Bob. L'image est tirée de GOOGLE MAPS. Le réel trajet emprunté par la fibre ne correspond à celui tracé ici.

4.4.5 Compensation de la biréfringence

Les qubits à 1532 nm transmis vers Bob sont, à la sortie du miroir dichroïque MD (cf. fig. 4.9), couplés dans l'axe lent d'une fibre à maintien de polarisation (représentée par un trait gras) orientée pour maximiser la transmission dans le cube polariseur C_A. Après C_A, les photons sont couplés dans la fibre 1 (unimodale standard). Cette fibre est ensuite connectée à une des fibres souterraines. Les fluctuations thermiques et les contraintes mécaniques appliquées sur la fibre souterraine induisent une biréfringence qui fluctue dans le temps. Or, l'ATU de Bob requiert une polarisation précise à son entrée pour fonctionner correctement.

10. « Optical time domain reflectometer ».

Pour éliminer les effets de la fluctuation de la biréfringence du lien, nous avons ajouté un système de stabilisation de la polarisation basé sur la succession de trames [171] représentées sur la fig. 4.11. Le système comporte deux trames nommées *trame de stabilisation* et *trame quantique*. Durant la *trame de stabilisation*, d'une durée de 0,4 s et répétée toutes les 10 secondes, la pompe est désactivée de sorte qu'aucune paire n'est créée. La diode laser DL_p génère alors une impulsion intense de 100 ms à 1536,47 nm. Cette impulsion est injectée dans une fibre à maintien de polarisation puis réfléchie à C_A de sorte que la polarisation de l'impulsion soit orthogonale à celle des qubits. Si on néglige la dispersion chromatique du lien, cette orthogonalité est préservée tout au long de la transmission vers Bob de sorte que l'impulsion peut servir de référence pour rectifier la polarisation des qubits. Cette rectification est réalisée à l'aide d'un stabilisateur de polarisation SP commercial (modèle PSY-101 de General Photonics) dont la polarisation à sa sortie peut être choisie par l'utilisateur. À l'arrivée du front montant de l'impulsion de référence, le SP est initialement désactivé. Le front montant franchit ensuite le SP, est partiellement réfléchi au cube polariseur C_B puis est détecté par le détecteur D_p. Cette détection déclenche alors une routine dans l'ordinateur qui active le SP durant 50 ms. À ce moment, le front descendant l'impulsion de référence n'a toujours pas franchi le SP et ce dernier utilise l'impulsion de référence pour compenser la biréfringence du lien et maximiser la transmission des qubits polarisés orthogonalement à l'impulsion de référence dans C_B. Le stabilisateur de polarisation SP est ensuite désactivé et la trame de stabilisation se termine. Elle est suivie par la *trame quantique* durant laquelle la pompe crée des paires intriquées pour une durée de 9,6 s. Le cycle est ensuite répété. Ce système de stabilisation combiné avec les trames est très stable et pouvait fonctionner durant une journée complète sans aucune difficulté.

4.4.6 Synchronisation et acquisition des données

Du côté d'Alice, les signaux créés par l'enregistrement d'un coup à S_+ ou à S_- sont mélangés dans le circuit de traitement Circ_A avec un signal de synchronisation provenant de l'horloge (*hor*) de la pompe. Ce circuit permet de générer trois signaux. Le premier, *det*, est présent uniquement lorsqu'un coup est enregistré à S_+ ou S_- et est synchrone avec *hor*. Le deuxième, $S_+ \vee S_-$, est le OU logique entre S_+ et S_- et est utilisé pour déterminer dans quelle fenêtre temporelle le coup a été enregistré. Le troisième, $S_- \wedge hor$, correspond au ET logique entre S_- et *hor* et est utilisé pour déterminer quel détecteur a enregistré le coup. Ainsi, la présence de ce signal indique que le coup provient de S_-, tandis que son absence indique qu'il provient de S_+. Ces signaux sont ensuite multiplexés dans le temps à l'aide du circuit MUX. Le signal multiplexé active la diode laser DL_s qui envoie ses impulsions dans la fibre 2, laquelle est ensuite connectée avec la deuxième fibre souterraine. Du côté de Bob,

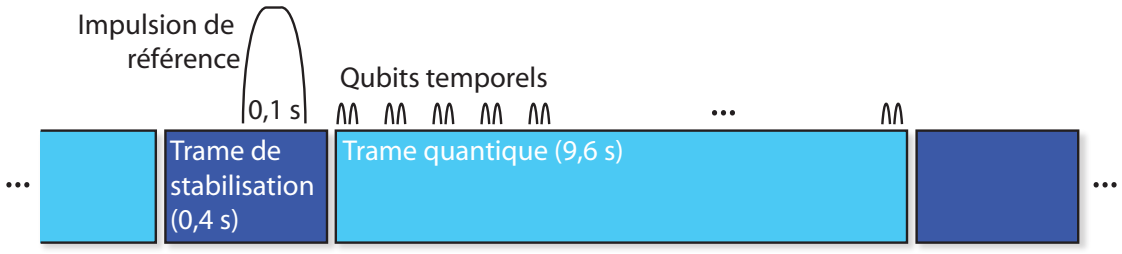

FIGURE 4.11 Séquence du système de stabilisation de la polarisation. Durant la *trame de stabilisation*, une impulsion de 0,1 s est utilisée comme référence pour compenser la biréfringence du lien. Ensuite, durant la *trame quantique*, les qubits photoniques à 1532 nm sont envoyés vers Bob.

les signaux sont d'abord détectés par D_s puis démultiplexés à l'aide du circuit DEMUX. Le signal *det* est ensuite utilisé pour activer les détecteurs I_+ et I_-. Autrement dit, Bob active ses détecteurs uniquement lorsqu'Alice a enregistré un coup. Les signaux I_+ et I_- émanant des coups enregistrés par les détecteurs de Bob sont mélangés avec les signaux « *gate-out* »[11] respectifs (notés « *g-out* » sur la fig. 4.9) dans le circuit Circ_B. Le signal sortant « *prêt* » est présent uniquement si les deux détecteurs de Bob ont émis un signal « *gate-out* » et est utilisé pour démarrer l'acquisition du convertisseur analogique-numérique temporel TDC-GPX qui mesure les délais entre le signal « start » est plusieurs signaux « stop » (cf. section 3.4.3). Cela nous assure que les statistiques ne sont pas biaisées par le temps mort des détecteurs InGaAs de Bob. Les autres sorties de Circ_B correspondent aux signaux I_+ et I_- et sont utilisés comme signaux « stop ». Les signaux $S_+ \vee S_-$ et $S_- \wedge hor$ sont également enregistrés comme signaux « stop ». L'acquisition et le traitement des données se fait en temps réel avec le logiciel LABVIEW utilisé conjointement avec des routines C++ conçues spécialement pour cette expérience. Ceci nous a permis d'enregistrer tous les coups survenant dans les fenêtres temporelles f_2 respectives d'Alice et de Bob. La largeur de cette dernière était variable entre 0,4 et 0,8 ns.

4.4.7 Montage sans la fibre souterraine

Le montage est considérablement simplifié lorsque les qubits ne sont pas transmis par la fibre souterraine. Premièrement, le système de stabilisation de la polarisation n'est pas nécessaire car la fibre à maintien de polarisation dans laquelle les qubits de Bob sont initialement couplés est directement connectée dans C_B (cf. fig. 4.9). Deuxièmement, les circuits

11. On rappelle que chaque détecteur InGaAs est équipé d'une sortie « gate-out » qui répète le signal d'activation externe du détecteur uniquement si celui-ci n'est pas à l'intérieur d'un temps mort de 10 µs causé par un coup antérieur (cf. section 3.4.2).

MUX et DEMUX du système de synchronisation ne sont pas nécessaires non plus car les signaux *det*, $S_+ \vee S_-$ et $S_- \wedge hor$ utilisés chez Bob proviennent directement du circuit Circ_A.

4.4.8 Ajustement du délai des interféromètres

Cette expérience nécessite que le délai de chaque interféromètre soit le même à une fraction du temps de cohérence des photons près. Ce dernier est égal à 0,27 ps (section 3.4.1), ce qui correspond à une longueur de cohérence de 81 µm. Pour ajuster les interféromètres, nous avons eu recours à la technique d'interférométrie à faible cohérence. Plus précisément, une source de lumière blanche ayant une longueur de cohérence de 5 µm était envoyée dans un interféromètre servant de référence et la sortie de cet interféromètre était envoyée dans l'interféromètre à ajuster. À l'aide d'un actuateur piézoélectrique, la longueur d'un des bras de l'interféromètre de référence pouvait varier de quelques longueurs d'onde. Lorsque la différence entre les délais des interféromètres est nulle, on observe une visibilité interférométrique de 50% dans le cas idéal. Ainsi, la longueur d'un des bras de l'interféromètre à ajuster est changée graduellement jusqu'à l'obtention d'une visibilité près de 50%. Ceci nous assure que le délai de chaque interféromètre est ajusté à la même valeur à 5 µm près. Cette technique est expliquée en détail dans les références [160, 172].

4.4.9 Une source d'intrication hybride

La combinaison de notre source d'intrication temporelle avec les deux ATU peut être interprétée comme une source d'intrication hybride où un qubit de polarisation à 812 nm est intriqué avec un qubit temporel à 1532 nm, ou vice versa. Elle peut également être interprétée comme une source d'intrication temporelle convertie en une source d'intrication en polarisation. En effet, chaque ATU peut être vu soit comme un analyseur temporel universel, soit comme un convertisseur de l'encodage temporel vers l'encodage en polarisation suivi d'un analyseur en polarisation. Par exemple, une source d'intrication hybride avec laquelle un qubit de polarisation à 812 nm transmis à l'air libre est intriqué avec un qubit temporel à 1532 nm transmis par une fibre serait obtenue en insérant un lien de transmission à l'air libre entre le convertisseur d'encodage de l'ATU d'Alice (compris dans la boîte régulée en température de la fig. 4.7) et l'analyseur de polarisation (formé par les composants Q3, D2, C2 et les détecteurs, cf. fig. 4.7).

4.5 Résultats expérimentaux

4.5.1 Histogrammes temporels des coups d'Alice et de Bob

Les coups enregistrés par Alice et Bob sont distribués dans trois pics séparés par 1,4 ns. La fig. 4.12-a montre l'histogramme temporel du signal $S_+ \vee S_-$ ainsi que les fenêtres f_0, f_1 et f_2. Seules les détections à l'intérieur de f_2 furent compilées. La séparation entre les différentes fenêtres est d'environ 1,4 ns, tel qu'attendu. La largeur de chaque pic est causé par le vacillement [12] des détecteurs au silicium et est approximativement égale à 400 ps. La fig. 4.12-b montre l'histogramme des détections à I_+ de Bob (celui de I_- est similaire) lorsque Bob était à l'UdeC superposé à celui où Bob était à SAIT. La largeur à mi-hauteur de chaque pic de l'histogramme à l'UdeC, approximativement égale à 160 ps, nous indique la valeur du vacillement des détecteurs InGaAs. Sur l'histogramme à SAIT, on observe un élargissement temporel marqué des pics. Ceci est causé principalement par la dispersion chromatique de la fibre souterraine, et potentiellement par le vacillement des circuits MUX et DEMUX qui s'ajoutent à celui des détecteurs. Cet élargissement temporel cause une superposition des pics qui, en principe, pourrait être éliminée en filtrant le spectre des photons de Bob pour ainsi s'affranchir de l'effet de la dispersion chromatique.

4.5.2 Visibilité de l'intrication

Dans le but de caractériser notre source et de démontrer l'universalité des ATU, nous avons mesuré la visibilité de l'intrication en balayant plusieurs grands cercles sur la sphère de Bloch. Plus précisément, trois configurations ont été testées.

Pour la première configuration, illustrée par la fig. 4.13-a, l'ATU d'Alice était positionné pour mesurer dans la base $\mathcal{B}_\times \equiv \{|+\rangle, |-\rangle\}$ et celui de Bob pour mesurer dans la base $\mathcal{B}_\times(\phi_B) \equiv \{|+\rangle_{\phi_B}, |-\rangle_{\phi_B}\}$. Puis, on faisait varier la phase ϕ_B en appliquant une tension V sur l'actuateur piézoélectrique de l'ATU de Bob (ceci est représenté par le plan ombragé). Cette configuration est identique à celle obtenue lorsqu'Alice et Bob utilisent chacun un *analyseur temporel standard* (fig. 2.2) contraint à projeter sur une base sur l'équateur de la sphère de Bloch. Nous avons mesuré la quantité p_{ab} définie comme la probabilité d'enregistrer un coup double à S_a et I_b conditionnelle à l'activation des détecteurs de Bob (ce signal d'activation est donné par le signal « *prêt* »), où $a, b \in \{+, -\}$ sont les résultats d'Alice et de Bob, respectivement. Cette probabilité est égale à $\tilde{P}^{11}_{ab}/p_1\eta_B$, où $\tilde{P}^{11}_{ab}$ est la probabilité d'un coup double par impulsion de pompe définie à l'éq. 4.22. Les fig. 4.13-b et c montrent les quatre courbes p_{ab} en fonction de la tension appliquée sur l'actuateur PZ lorsque Bob était à l'UdeC.

12. « Jitter ».

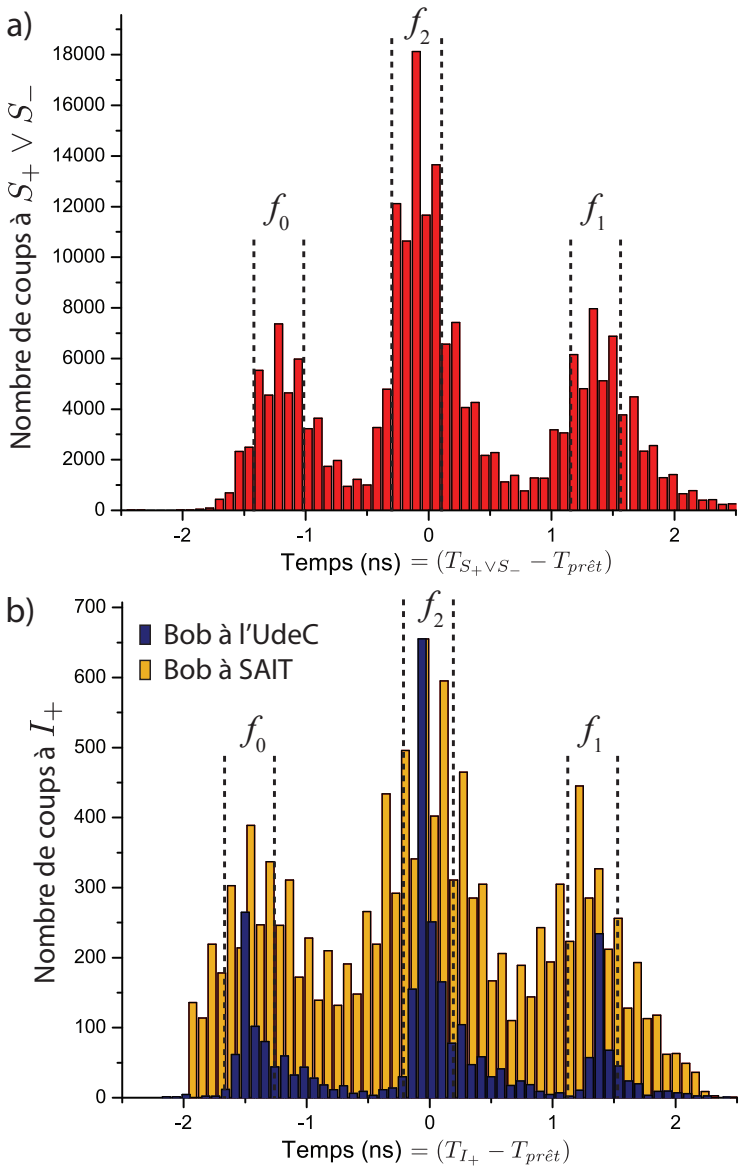

FIGURE 4.12 Histogrammes des signaux $S_+ \vee S_-$ et I_+ enregistrés par le convertisseur analogique-numérique temporel TDC-GPX. a) Histogramme temporel du signal $S_+ \vee S_-$. Le temps en abscisse, $T_{S_+ \vee S_-} - T_{prêt}$, correspond à la différence entre le temps du signal « stop » provenant de $S_+ \vee S_-$ et le temps du signal « start » provenant de *prêt*. L'origine du temps a été centrée sur la fenêtre f_2. b) histogramme temporel des coups à I_+ lorsque Bob était à l'UdeC et lorsque Bob était à SAIT. Le temps en abscisse correspond à $T_{I_+} - T_{prêt}$.

On observe clairement la variation sinusoïdale prédite par l'éq. 4.23. Nous avons également tracé le nombre de coups mesurés à S_+ (fig. 4.13-b) et à S_- (fig. 4.13-c). Comme ces courbes sont constantes, cela nous assure que la variation de p_{ab} n'est pas causée par une variation du nombre de coups à S_+ et S_-. L'incertitude sur chaque point est calculée en supposant une

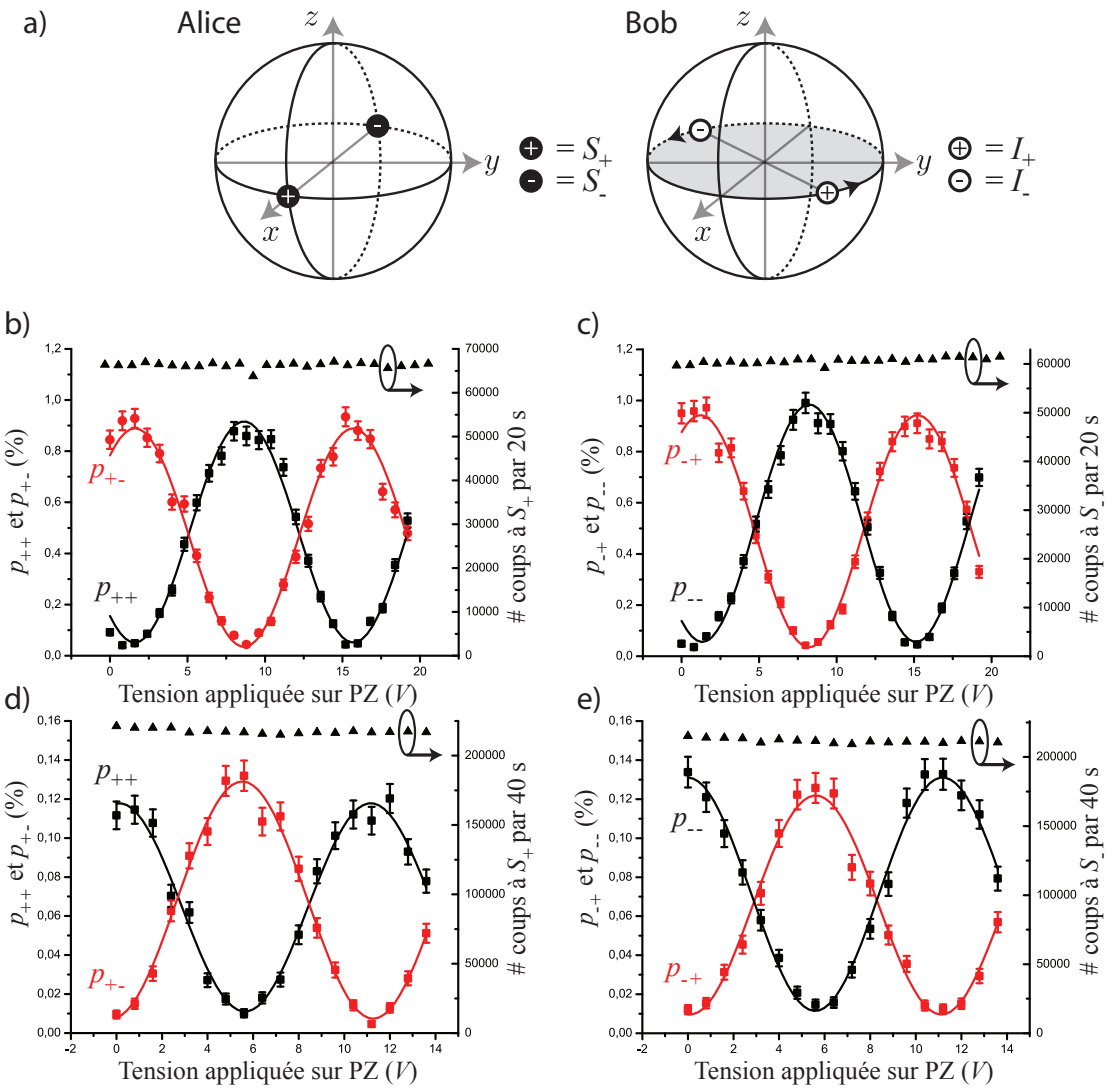

FIGURE 4.13 a) Première configuration utilisée pour mesurer la visibilité de l'intrication. b) et c) Courbes p_{ab} pour Bob à l'UdeC. d) et e) Courbes p_{ab} pour Bob à SAIT.

distribution binomiale du nombre total de coups enregistrés. La visibilité moyenne calculée à partir du lissage de chaque courbe est égale à $(91{,}0 \pm 2{,}9)\%$, où l'incertitude est calculée par le lissage. Les fig. 4.13-d et e montrent les résultats lorsque Bob était à SAIT. La visibilité moyenne est de (85,4±3,3)%. La diminution de la visibilité est entièrement due à la diminution du rapport signal/bruit, tel que discuté plus loin.

Pour la deuxième configuration, illustrée par la fig. 4.14-a, les ATU d'Alice et de Bob étaient initialement positionnés pour mesurer dans la base $\mathcal{B}_+ = \{|t_0\rangle, |t_1\rangle\}$. Puis, la lame demi-onde D2 de l'ATU d'Alice (cf. fig. 4.7) était tournée pour balayer le grand cercle x-z (contour de la zone ombragée). Cette configuration n'a jamais été testée auparavant avec

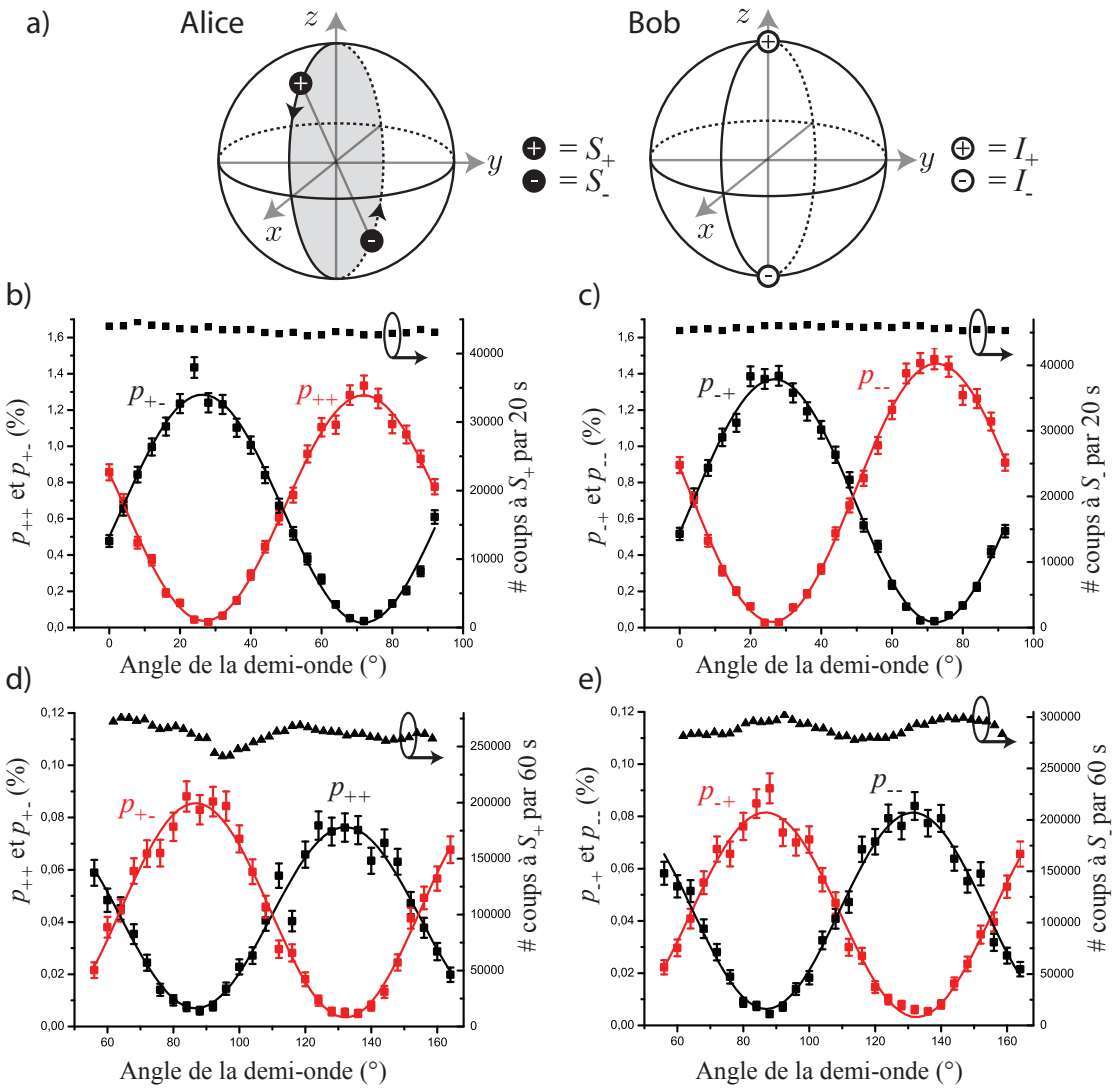

FIGURE 4.14 a) Deuxième configuration utilisée pour mesurer la visibilité de l'intrication. b) et c) Courbes p_{ab} pour Bob à l'UdeC. d) et e) Courbes p_{ab} pour Bob à SAIT.

l'intrication temporelle. La visibilité moyenne avec Bob à l'UdeC est de $(95{,}6 \pm 1{,}9)\%$. Celle-ci est plus élevée que celle de la première configuration. Au moment d'écrire cette thèse, l'explication de cette différence reste encore à établir mais nous suspectons que la dispersion chromatique de la fibre dans l'ATU de Bob y joue un rôle. Lorsque Bob était à SAIT, la visibilité moyenne diminue à $(88{,}4 \pm 3{,}2)\%$ en raison de la diminution du rapport signal/bruit (fig. 4.14-d et e).

Pour la troisième configuration, illustrée par la fig. 4.15-a, l'ATU de Bob était positionné pour mesurer dans la base $\mathcal{B}_+$ et celui d'Alice pour mesurer initialement dans la base $\mathcal{B}_\times$ sélectionnée à l'aide de la lame quart d'onde Q3 et de la demi-onde D2 (cf. fig. 4.7). Puis, la

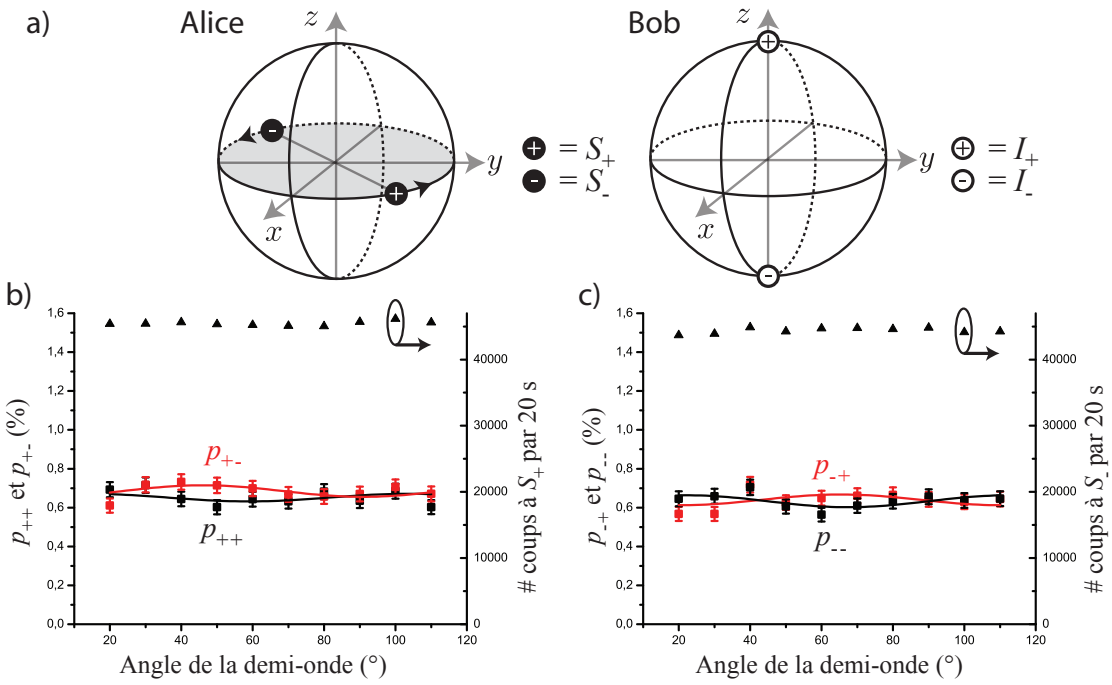

FIGURE 4.15 a) Troisième configuration utilisée pour mesurer la visibilité de l'intrication. b) et c) Courbes p_{ab} pour Bob à l'UdeC.

demi-onde était tournée pour balayer la base $\mathcal{B}_\times(\theta)$, où l'angle de l'axe lent de la demi-onde est $\theta/4$. Les deux bases sont mutuellement non biaisées, indépendamment de la valeur de θ. Par conséquent, la visibilité de l'intrication devrait être nulle. C'est ce que nous observons sur les fig. 4.15-b et c (Bob à l'UdeC). La visibilité des lissages est inférieure à 5%.

Le tableau 4.1 résume les résultats obtenus. Pour Bob à l'UdeC, la visibilité est limitée principalement par l'alignement imparfait de l'optique. Pour arriver à cette conclusion, la contribution des coups doubles accidentels entre Alice et Bob a été estimée. Les coups doubles accidentels proviennent de tous les coups doubles dont au moins un des deux coups ne provient pas d'un qubit photonique. Or, la probabilité d'un coup sombre aux détecteurs au

TABLEAU 4.1 Résultats de la mesure de la visibilité de l'intrication.

Conf.	Base de Alice	Base de Bob	Cercle balayé	V (Bob à l'UdeC)	V (Bob à SAIT)
1	$B_\times$	$B_\times$	x-y par Bob	$(91{,}0 \pm 2{,}9)\%$	$(85{,}4 \pm 3{,}3)\%$
2	B_+	B_+	x-z par Alice	$(95{,}6 \pm 1{,}9)\%$	$(88{,}4 \pm 3{,}2)\%$
3	$B_\times$	B_+	x-y par Alice	$< 5\%$	$--$

silicium d'Alice est si faible ($\approx 2{,}5 \times 10^{-7}$ par 5 ns par détecteur) qu'ils contribuent de façon négligeable. Seuls les coups doubles accidentels causés par un photon chez Alice et un coup sombre chez Bob contribuent significativement à la diminution de la visibilité. Pour estimer cette contribution, nous avons bloqué le faisceau de Bob et obtenu $p_{ab}^{\text{acc}} \approx 2{,}9 \times 10^{-5}$, ce qui est au moins dix fois inférieur au minimum des courbes b et c de la fig. 4.14. Leur contribution à la réduction de la visibilité est donc faible. Ce n'est plus le cas lorsque Bob était à SAIT. En effet, les pertes supplémentaires introduites par le lien et le système de compensation de la biréfringence (environ 10 dB) réduisent le rapport signal sur bruit ce qui, en retour, diminue la visibilité observée. Or, en soustrayant la contribution des coups doubles accidentels des visibilités obtenues avec Bob à SAIT, on retrouve celles obtenues à l'UdeC. Ceci démontre que le degré d'intrication des états créés n'est pas affecté par la transmission par la fibre souterraine. Comme la visibilité est supérieure ou égale à 85%, cette source peut être utilisée pour la DQC car la limite inférieure pour accomplir cette tâche est $V > 78\%$ (cf. section 4.2.1).

La stabilité de notre système dépend de la stabilité de la phase relative entre les trois interféromètres utilisés. En laissant dériver les courbes p_{ab} dans le temps, nous avons observé que la phase de celles-ci dérivait d'au plus $\pi/10$ sur 10 minutes. Cette durée a été choisie comme la durée maximale de chaque mesure. Cette limite peut être éliminée en verrouillant la phase de tous les interféromètres à l'aide d'un laser à fréquence stabilisée utilisé comme sonde.

4.5.3 Tests de l'inégalité de Bell-CHSH

Nous avons étudié la non-localité de notre source d'intrication à l'aide des ATU. Spécifiquement, nous désirions vérifier que la valeur du paramètre S est invariante par rotation des bases de mesures ce qui, au meilleur de notre connaissance, n'a jamais été étudié avant ces travaux. Une telle vérification basée sur une source d'intrication temporelle nécessitait l'utilisation des ATU. Pour réaliser cette vérification, nous avons mesuré l'inégalité de Bell-CHSH avec quatre configurations illustrées à la fig. 4.16. La configuration 1 correspond à ce qui a déjà été réalisé à l'aide d'analyseurs temporels standards contraints à projeter sur une base donnant sur l'équateur de la sphère de Bloch. Les trois autres configurations nécessitent les ATU. En particulier, les bases d'Alice (Bob) de la configuration 2 (3) correspondent à projeter sur des états temporels dont les amplitudes des composantes $|t_0\rangle$ et $|t_1\rangle$ n'ont pas le même poids. C'est également le cas pour les bases d'Alice et de Bob de la configuration 4. Au meilleur de notre connaissance, la configuration 4 n'a jamais été testée auparavant.

Pour mesurer correctement le paramètre S de chaque configuration proposée, il faut ajuster la phase des interféromètres d'Alice et de Bob. Comme nous l'avons mentionné, cela

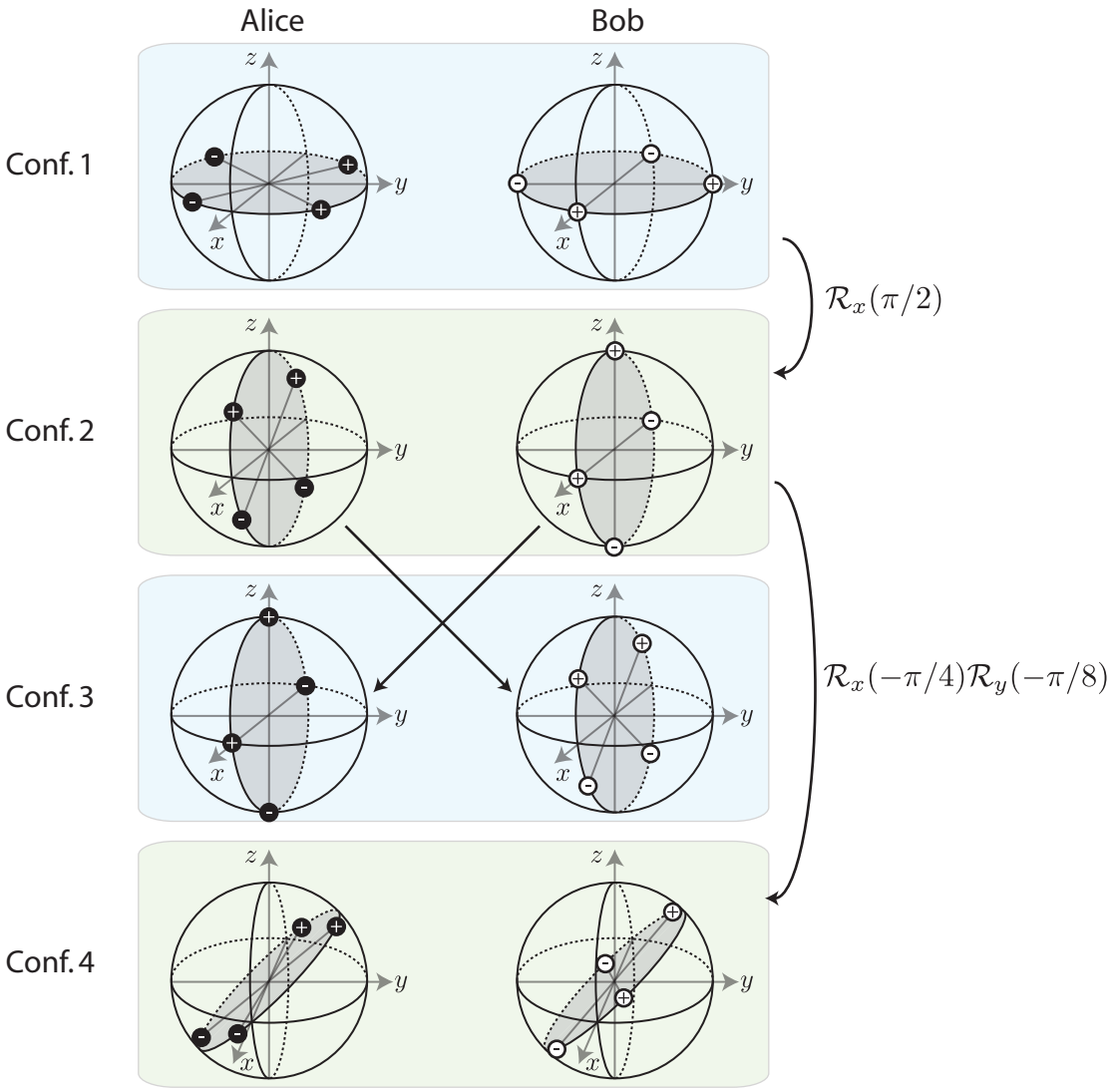

FIGURE 4.16 Configurations utilisées pour tester l'inégalité de Bell-CHSH. La transformation pour passer d'une configuration à la suivante est indiquée. La notation $\mathcal{R}_x(\alpha)$ signifie une rotation d'un angle α autour de l'axe x, etc.

pourrait se faire en verrouillant les interféromètres à l'aide d'un laser à fréquence stabilisée utilisé comme référence. Cela est souhaitable mais pas nécessaire. Pour comprendre ceci, considérons l'état conjoint des deux qubits dans la fenêtre f_2 juste après les cubes C1 (fig. 4.7) et C5 (fig. 4.8) des ATU d'Alice et de Bob. Cet état peut s'écrire comme $\frac{1}{\sqrt{2}}(|HH\rangle + \mathrm{e}^{-i(\varphi_A+\varphi_B)}|VV\rangle)$, où les phases φ_A et φ_B sont causées par les interféromètres d'Alice et de Bob, respectivement. Supposons que l'ATU d'Alice est orienté pour mesurer dans la base $A_1 = \{|+\rangle, |-\rangle\}$ et celui de Bob pour mesurer dans la base $B1 = \{|+\rangle_\beta, |-\rangle_\beta\}$, où la phase β est déterminée par le contrôleur de polarisation et est inconnue (cf. section 4.4.2).

Le calcul du coefficient de corrélation E_{11} présenté à la section 4.2.1 et aboutissant à l'éq. 4.26 peut alors être repris en tenant compte des phases φ_A, φ_B et β ci-haut. On peut montrer que, dans ce cas, on obtient $E_{11} = V\cos(\varphi_A + \varphi_B - \beta)$. Ainsi, on peut correctement sélectionner la première base de mesure de Bob en faisant varier φ_B jusqu'à l'obtention de $E_{11} = V/\sqrt{2}$, ce qui indique que $\varphi_A + \varphi_B - \beta = \pm\frac{\pi}{4}$. Lorsque c'est le cas, on poursuit avec les mesures des trois autres coefficients de corrélation. La justesse du paramètre S obtenu dépend de cet alignement initial. Si cet alignement n'est pas fait correctement, la valeur de S ne peut qu'en être diminuée. Le tableau 4.2 donne en exemple les quatre valeurs des coefficients E_{ij} obtenues lors d'une mesure dans la configuration 1 lorsque Bob était soit à l'UdeC, soit à SAIT.

En considérant les valeurs obtenues pour la visibilité de l'intrication (tableau 4.1), nous nous attendions à obtenir une valeur $2{,}57 \lesssim S_U \lesssim 2{,}70$ lorsque Bob était à l'UdeC et $2{,}40 \lesssim S_S \lesssim 2{,}49$ lorsque Bob était à SAIT. Les valeurs obtenues sont présentées au tableau 4.3. Elles correspondent aux valeurs attendues. Ces valeurs sont la moyenne de plusieurs mesures. On note que l'écart-type de chaque valeur était limitée par le temps de mesure, c'est-à-dire

TABLEAU 4.2 Coefficients E_{ij} obtenus avec la configuration 1 avec Bob à l'UdeC ou à SAIT. En tenant compte de la visibilité correspondante (tableau 4.1), la valeur cible de E_{11} utilisée pour l'alignement initial de la phase, donnée par $V/\sqrt{2}$, est également présentée.

	Bob à l'UdeC	Bob à SAIT
Cible de E_{11}	0,643	0,603
$E_{11} \pm \Delta E_{11}$	$0{,}663 \pm 0{,}034$	$0{,}576 \pm 0{,}039$
$E_{12} \pm \Delta E_{12}$	$-0{,}672 \pm 0{,}034$	$-0{,}601 \pm 0{,}037$
$E_{21} \pm \Delta E_{12}$	$0{,}586 \pm 0{,}037$	$0{,}475 \pm 0{,}044$
$E_{22} \pm \Delta E_{22}$	$0{,}695 \pm 0{,}033$	$0{,}789 \pm 0{,}030$

TABLEAU 4.3 Résultats de la violation de l'inégalité de Bell-CHSH pour chaque configuration de la fig. 4.16. S_U (S_S) est le paramètre S obtenu lorsque Bob était à l'UdeC (SAIT) et σ_U (σ_S) est l'écart-type statistique de la mesure correspondante. Les colonnes $\times\sigma_U$ et $\times\sigma_S$ indiquent la séparation entre la borne locale $S = 2$ et la valeur mesurée en termes du nombre d'écart-type. Chaque mesure de S_U (S_S) nécessitait 160 s (480 s) de temps de mesure.

Conf.	$S_U \pm \sigma_U$	$(\times\sigma_U)$	$S_S \pm \sigma_S$	$(\times\sigma_S)$
1	$2{,}65 \pm 0{,}09$	7,7	$2{,}44 \pm 0{,}15$	2,9
2	$2{,}60 \pm 0{,}08$	7,5	$2{,}40 \pm 0{,}15$	2,7
3	$2{,}65 \pm 0{,}09$	7,5	$2{,}39 \pm 0{,}15$	2,6
4	$2{,}60 \pm 0{,}1$	6	$2{,}39 \pm 0{,}15$	2,7

10 minutes ou moins, pour assurer que le système était stable et que la dérive n'aurait pu fausser les résultats.

4.6 Discussion

L'étude de notre source d'intrication temporelle a plusieurs conséquences.

- Premièrement, elle démontre bien le caractère universel des ATU utilisés.
- Deuxièmement, elle démontre que le degré d'intrication des états créés n'est pas affecté de façon significative par la transmission par fibre souterraine de 12,4 km et que notre source peut directement être utilisée pour la distribution quantique de clés.
- Troisièmement, cette étude met clairement en évidence que la valeur du paramètre S est invariante par rotation du grand cercle contenant les bases de mesure utilisées dans un test de l'inégalité de Bell-CHSH.
- Finalement, la source créée peut être interprétée comme une source d'intrication hybride entre un qubit de polarisation à 812 nm et un qubit temporel à 1532 nm ou vice versa. Cela démontre bien que l'intrication est un concept indépendant des degrés de liberté utilisés pour encoder l'intrication.

L'importance des ATU se reflète de trois façons. Premièrement, l'ATU est un nouvel outil utile à l'implémentation de nouveaux protocoles de communication quantique tel que le démontrent les travaux présentés au chapitre 5. Deuxièmement, l'utilisation des ATU permet en principe de tester une inégalité de Leggett et l'inégalité « élégante » avec une source d'intrication temporelle. Ceci nécessite de mesurer dans des bases explorant toutes les dimensions de la sphère de Bloch, ce qui n'était pas possible avant l'introduction de ces ATU. Finalement, l'utilisation d'un ATU comme convertisseur d'encodage peut s'avérer utile à la création d'une interface quantique entre différents types de lien de transmission de l'intrication photonique. Cette source est donc utile à la communication quantique en général.

Chapitre 5

Pile ou face quantique

Dans les chapitres précédents, nous avons présenté différentes avancées expérimentales, culminant vers la réalisation d'une source photonique d'intrication temporelle. Dans ce chapitre, nous nous concentrons sur une application de la communication quantique, le *pile ou face quantique*. Nous présentons le premier protocole de pile ou face quantique *tolérant aux pertes*. Ceci règle un problème important car, avant ces travaux, aucun protocole de pile ou face quantique n'était en mesure de tolérer une perte de grandeur arbitraire sur le canal de transmission. Nous discutons ensuite des conséquences du bruit dans un montage réaliste et présentons une nouvelle tâche que nous nommons *pile ou face séquentiel*, qui est basée sur l'application répétée de notre protocole de pile ou face quantique. Cette tâche est telle que sa sécurité n'est pas compromise même en présence de bruit. Finalement, nous présentons la première implémentation d'un protocole de pile ou face tolérant aux pertes et de son utilisation pour le pile ou face séquentiel. Cette implémentation est basée sur la source d'intrication temporelle que nous avons présentée au chapitre 4.

Les sections 5.1 à 5.7 présentent notre protocole et les sections 5.8 à 5.13 discutent de différents aspects reliés à l'implémentation de ce protocole ainsi que de l'implémentation elle-même.

5.1 Introduction

La primitive cryptographique de *pile ou face*[1] a été introduite par Manuel Blum en 1981 dans les termes suivants : « Alice and Bob [...] have just divorced, live in different cities, want to decide who gets the car » [50]. Ils s'entendent sur le fait que la meilleure chose à faire est de tirer à pile ou face, mais ils ne se font pas confiance et ne peuvent s'entendre sur le choix d'un tiers de confiance[2] pour tirer à pile ou face à leur place. De façon plus générale, un protocole de pile ou face peut être utilisé lorsque deux joueurs doivent générer un bit aléatoire commun. Ceci doit demeurer vrai même si un des joueurs était tenté de manipuler le protocole pour biaiser le résultat. Le pile ou face quantique et la distribution quantique

1. « Coin flipping » ou « coin tossing ».
2. « Trusted third party ».

de clés (DQC) diffèrent fondamentalement en raison de la nature des joueurs. Pour la DQC, Alice et Bob sont des collaborateurs et l'adversaire potentiel est une tierce partie. Par contre, pour le pile ou face, Alice et Bob sont potentiellement des adversaires et un des deux joueurs peut tenter de tricher. Cette différence rend le pile ou face considérablement plus difficile à réaliser que la DQC.

Le protocole original de Blum est *asynchrone*, c'est-à-dire qu'il consiste en une séquence de rondes durant lesquelles les deux joueurs s'échangent des messages (classiques) à tour de rôle. La sécurité du protocole repose sur la supposition que la factorisation de grands nombres en facteurs premiers est difficile. Dans le monde quantique, cette supposition est cependant fausse en raison de l'algorithme de Shor [75]. Il est cependant possible qu'un protocole basé sur des fonctions à sens unique soit immunisé contre un ordinateur quantique. Néanmoins, tout protocole asynchrone n'utilisant que la transmission de messages classiques est tel qu'un des deux joueurs, s'il était doté d'une puissance de calcul illimitée, aurait la possibilité de complètement biaiser le résultat. Dans le meilleur des cas, la sécurité d'un tel protocole est donc basée sur des hypothèses calculatoires non prouvées.

Des protocoles de pile ou face inconditionnellement sécuritaires existent dans le modèle *synchrone* où les joueurs envoient leurs messages simultanément, ce qui assure leur indépendance. Ces protocoles sont qualifiés de *relativistes* car la relativité restreinte doit être invoquée pour empêcher Alice d'attendre l'arrivée du message de Bob avant de faire son choix en conséquence (et vice versa). La sécurité des protocoles relativistes dépend directement de la distance entre les joueurs et ces derniers doivent être certains que l'autre joueur est réellement situé à la position où il prétend être. Cette tricherie peut être évitée si chaque joueur a un partenaire honnête capable de certifier la position de l'autre joueur [173]. Cette nécessité rend les protocoles relativistes difficiles à implémenter. Dans le reste de ce chapitre, nous ne considérerons que les protocoles de pile ou face asynchrones.

Lorsqu'on permet à Alice et Bob d'échanger de l'information quantique, on parle alors de *pile ou face quantique*. Ce type de protocole a été étudié pour la première fois par C. H. Bennett et G. Brassard en 1984 [3] et la grande majorité des protocoles asynchrones subséquents suivent un canevas similaire à celui proposé par BB84. L'idée fondamentale est qu'il est possible de dissimuler un bit dans un état quantique. Plus précisément, Alice peut dissimuler un bit x dans un état quantique ρ_x et l'envoyer à Bob. Cette dissimulation est telle qu'il est impossible pour Bob de deviner avec certitude la valeur de x en mesurant ρ_x. Par la suite, Bob peut envoyer un bit aléatoire b à Alice. Puis, Alice révèle la description de l'état qu'elle a envoyé, ce qui permet à Bob de mesurer l'état d'une façon lui permettant de vérifier si la description qu'Alice a donné est cohérente avec l'état qu'il a reçu. Si cette mesure donne un résultat incohérent avec la description, Alice se fait prendre à tricher. Si elle ne se fait pas

prendre à tricher, le résultat du pile ou face est $c = x \oplus b$, où « $\oplus$ » est la somme modulo 2 des bits x et b.

Le protocole de pile ou face quantique que C. H. Bennett et G. Brassard ont présenté, que nous nommerons le protocole BB84, [3] n'est malheureusement pas sécuritaire contre une Alice malhonnête utilisant l'intrication. Cette restriction laissait toutefois intacte la possibilité de construire un protocole parfait de pile ou face. Par protocole parfait, on entend un protocole dont le résultat c est impossible à biaiser par un tricheur éventuel. La preuve que ce protocole parfait est impossible à construire fut donnée en 1998 par H.-K. Lo et H. F. Chau [51] et par D. Mayers, L. Salvail et Y. Chiba-Kohno [52]. Malgré tout, si un protocole parfait n'existe pas, existe-t-il un protocole capable de faire mieux que tout ce qui est possible classiquement ?

Pour préciser cette question, on dira que le *biais* d'un joueur est ε s'il existe un stratégie de triche lui permettant d'obtenir le résultat désiré avec une probabilité $\frac{1}{2} + \varepsilon$. Ceci suppose que le résultat désiré peut être tant le bit 0 que le bit 1. On suppose aussi que l'autre joueur suit le protocole de façon honnête. Cette définition est *inconditionnelle* car on suppose que le tricheur potentiel a accès à une puissance de calcul illimitée ainsi qu'à une technologie limitée uniquement par les lois de la physique. Le *biais* d'un protocole est la plus grande valeur possible de ε qui est telle que le biais d'au moins un des joueurs est ε. Un protocole parfait, s'il existait, aurait un biais de 0. D'autre part, un protocole ayant un biais de 0,5 est considéré comme *complètement brisé*. Ainsi, tous les protocoles classiques et le protocole BB84 sont complètement brisés. La question du paragraphe précédent peut donc être reformulée ainsi : existe-t-il un protocole de pile ou face quantique ayant un biais inférieur à 0,5 ?

Le premier protocole de la sorte a été découvert en 2000 par D. Aharonov, A. Ta-Shma, U. Vazirani et A. C.-C. Yao [174]. Ils ont montré que leur protocole, que nous nommerons le protocole ATVY, a un biais d'au plus $\sqrt{2} - 1 < 0{,}42$ [174]. Suite à cette découverte, R. W. Spekkens et T. Rudolph ont prouvé que le biais du protocole ATVY est en réalité égal à $\sqrt{2}/4 < 0{,}36$ [175]. Dans le même article, R. W. Spekkens et T. Rudolph ont également découvert un protocole ayant un biais $(\sqrt{5} - 1)/4 < 0{,}31$. Ce biais correspond à la plus petite valeur possible d'un protocole où un seul qubit est échangé [176].

En 2001, A. Ambainis [177] et, indépendamment, R. W. Spekkens et T. Rudolph [176], ont découvert des protocoles ayant un biais de 0,25. La réduction du biais sous la barre de 0,31 nécessite la transmission d'un qutrit dans le premier cas et d'un qubit et de deux qutrits dans le deuxième cas. Puis, en 2003, A. Kitaev a montré que pour tout protocole quantique, le biais doit être supérieur ou égal à $(\sqrt{2} - 1)/2 \approx 0{,}21$ [53]. Ce n'est que tout récemment qu'un protocole dont le biais est arbitrairement près de la borne de Kitaev a été découvert par A. Chailloux et I. Kerenidis [178]. D'un point de vue pratique, ce protocole est très complexe

3. À ne pas confondre avec le protocole de DQC présenté dans le même article et portant le même nom.

car il nécessite un nombre illimité de rondes pour que le biais approche cette borne.

Malgré les succès théoriques du pile ou face quantique, plusieurs problèmes techniques intrinsèques à leur implémentation existent, tel que discuté par J. Barrett et S. Massar [54]. Plus précisément, ceux-ci décrivent comment l'implémentation d'un protocole de pile ou face quantique dans un scénario réaliste, où les imperfections du montage causent du bruit dans les mesures ainsi que des pertes de transmission, est problématique. Pour cette raison, ils ont étudié une autre tâche, soit la *génération d'une chaîne de bits aléatoires*, au lieu du pile ou face quantique. Or, comme cette tâche peut être réalisée avec des méthodes purement classiques [179], toute approche quantique est beaucoup moins intéressante.

Cette tâche n'est cependant pas intéressante du point de vue de la cryptographie quantique car le même but peut être atteint à l'aide de méthodes purement classiques [179].

Dans un article ultérieur, A. T. Nguyen, J. Frison, K. Phan Huy et S. Massar (NFPM) ont présenté une implémentation d'un protocole qui n'est pas complètement brisé en présence de pertes sur le canal [180]. Cette implémentation est cependant sévèrement limitée par le fait qu'Alice est capable de choisir le résultat avec une probabilité pratiquement égale à 100% (99,71% pour être précis), et ce, même si la perte sur le canal reliant la sortie du laboratoire d'Alice à l'entrée du laboratoire de Bob est négligeable.

Pour être utile en pratique, nous croyons qu'un protocole doit être *tolérant aux pertes*, ce que nous définissons comme un protocole dont le biais est indépendant de la grandeur des pertes. Le protocole de NFPM n'est pas tolérant aux pertes car son biais tend vers 0,5 à mesure que les pertes augmentent ; ceci est, en pratique, inévitable lorsque la distance entre Alice et Bob augmente. Cela ouvre également la porte à une attaque où Alice gonfle artificiellement les pertes du canal dans le but d'augmenter le biais du protocole. Ce protocole est donc brisé *de facto*. Ce point est discuté en détail à la section 5.10.

Dans ce chapitre, nous considérons d'abord le problème des pertes sur le canal de transmission. Ces pertes comprennent toutes les pertes optiques du canal entre Alice et Bob et tiennent aussi compte du rendement quantique inférieur à 1 des détecteurs utilisés. Tous les protocoles mentionnés ci-haut, exception faite du protocole NFPM, sont complètement brisés en la présence de pertes. Ceci demeure vrai même si le bruit est nul. Nous présentons le premier protocole de pile ou face quantique tolérant aux pertes. Nous prouvons que le protocole peut être *équilibré*, ce qui signifie que les biais d'Alice et de Bob sont égaux, en l'occurrence 0,4, et que ce biais est indépendant de la grandeur des pertes de transmission.

Tout au long de ce chapitre, nous n'analysons que des scénarios où soit les deux joueurs sont honnêtes, soit un des joueurs triche. Nous ne considérons pas le scénario où les deux joueurs trichent parce que le but du protocole est de protéger le ou les joueurs honnêtes et pas le ou les tricheurs. Malgré cela, la question reste intéressante et une discussion est présentée

dans notre article [181].

Les sections qui suivent sont divisées de la façon suivante. Tout d'abord, nous décrivons à la section 5.2 le protocole de pile ou face quantique BB84 et nous expliquons pourquoi il est complètement brisé lorsqu'Alice triche en utilisant l'intrication. Ceci nous sera utile pour introduire le canevas de notre protocole tolérant aux pertes. Ensuite, la section 5.3 présente le protocole ATVY et le protocole d'Ambainis et, à la section 5.4, nous montrons pourquoi ces protocoles sont complètement brisés dès que la perte du canal n'est plus nulle. De plus, nous montrons que ce problème est intrinsèquement impossible à corriger dans le cas du protocole d'Ambainis en raison de l'existence des mesures concluantes, lesquelles sont présentées à la section 5.5. Dans la section 5.6, nous montrons comment on peut s'inspirer des protocoles BB84 et ATVY pour obtenir un nouveau protocole tolérant aux pertes et nous présentons une analyse de sa sécurité. Finalement, la section 5.7 présente quelques problèmes ouverts.

5.2 Protocole BB84

Nous présentons ici une version simplifiée du protocole de pile ou face quantique BB84 et une attaque permettant de le briser à l'aide de l'intrication. Nous supposons d'abord que les pertes et le bruit sont nuls. On définit les « états BB84 » :

$$\left.\begin{array}{l} |\psi_{0,0}\rangle = |0\rangle \\ |\psi_{0,1}\rangle = |1\rangle \end{array}\right\} \; x = 0$$
$$\left.\begin{array}{l} |\psi_{1,0}\rangle = |+\rangle \\ |\psi_{1,1}\rangle = |-\rangle \end{array}\right\} \; x = 1 \tag{5.1}$$

Nous dirons de l'état $|\psi_{x,a}\rangle$ que x est la *base* et que a est le *bit*. On définit ensuite les bases de mesures

$$\mathcal{B}_x = \{|\psi_{x,0}\rangle, |\psi_{x,1}\rangle\}, \tag{5.2}$$

où $x \in \{0,1\}$. Les étape du protocole honnête sont les suivantes :

1. Alice prépare un des quatre états $|\psi_{x,a}\rangle$ où la base x et le bit a sont choisis au hasard. Elle envoie cet état à Bob.
2. Bob choisit $\hat{x} \in \{0,1\}$ au hasard et mesure le qubit reçu dans la base $\mathcal{B}_{\hat{x}}$. Soit $\hat{a}$, le résultat obtenu par Bob.
3. Bob envoie un bit aléatoire b à Alice.
4. Alice révèle la base x et le bit a qu'elle a utilisés.

5. Si $x = \hat{x}$ et $a \neq \hat{a}$, Bob déclare une erreur, traite Alice de tricheuse et fait avorter le protocole. Si $x \neq \hat{x}$, Bob n'est pas en mesure de vérifier l'honnêteté d'Alice et le protocole continue.
6. Si le protocole n'a pas avorté, le résultat du pile ou face est $c = x \oplus b$.

Dans ce protocole, Bob ne peut tout simplement pas tricher. La meilleure stratégie qu'il puisse adopter est de tenter de deviner la base x d'Alice avant de décider de la valeur du bit b à envoyer à l'étape 3 pour ainsi obtenir le résultat $x \oplus b$ désiré. Or, a est un bit aléatoire. Ainsi, l'état ρ_x reçu par Bob à l'étape 1 est soit $\rho_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, soit $\rho_1 = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$. Comme $\rho_0 = \rho_1$, il est impossible pour Bob d'obtenir quelque information que ce soit sur la valeur de x et le mieux qu'il puisse faire est de choisir b au hasard.

Cet avantage du protocole BB84 n'est pas symétrique. En effet, Alice peut briser le protocole (c'est-à-dire obtenir un biais de 0,5) sans même risquer de se faire prendre à tricher en utilisant l'intrication [3]. Cette attaque se nomme *attaque EPR*. Soit c, le résultat désiré par Alice. Au lieu d'envoyer un des états BB84 à l'étape 1, Alice envoie la moitié d'une paire de qubits intriqués dans l'état $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et garde l'autre moitié avec elle. Pour obtenir le résultat c désiré avec certitude, Alice mesure dans la base $x = b \oplus c$ et déclare avoir envoyé l'état $|\psi_{x,a}\rangle$, où a est le résultat de sa mesure. Comme $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$, on voit directement qu'à chaque fois qu'Alice et Bob mesurent leurs moitiés respectives dans la même base $\mathcal{B}_x = \mathcal{B}_{\hat{x}}$, ils obtiendront le même bit $a = \hat{a}$. Lorsque $x \neq \hat{x}$, Bob doit accepter le bit d'Alice. Ainsi, Alice peut déclarer la base x de son choix sans jamais se faire prendre à tricher.

Quelques années plus tard, D. Mayers [182] et, indépendamment, H.-K Lo et H. F. Chau [183] ont montré que l'attaque EPR est toujours possible pour un protocole de pile ou face quantique suivant le canevas du protocole BB84 lorsque $\rho_0 = \rho_1$, où ρ_0 (ρ_1) est le mélange statistique codant le bit $x = 0$ ($x = 1$) à l'étape 1.

5.3 Protocole ATVY et protocole d'Ambainis

5.3.1 Protocole ATVY

Dans le but d'éviter l'attaque EPR, D. Aharonov, A. Ta-Shma, U. Vazirani et A. C.-C. Yao [174] ont introduit un protocole pour lequel $\rho_0 \neq \rho_1$. De plus, dans le but de minimiser le biais du protocole, ils ont modifié l'ordre des étapes du protocole BB84 de sorte que Bob mesure l'état reçu uniquement après qu'Alice ait révélé l'état qu'elle a envoyé (ou qu'elle prétend avoir envoyé). De cette façon, Bob mesure toujours dans la base contenant l'état déclaré par Alice, ce qui augmente la probabilité qu'elle se fasse prendre à tricher (lorsque c'est le cas).

Le biais de ce protocole est de $\sqrt{2}/4 < 0{,}36$ [176].

5.3.2 Protocole d'Ambainis

Pour réduire le biais à 0,25, A. Ambainis a dû utiliser des qutrits au lieu de qubits. Plus précisément, les états utilisés sont :

$$\left.\begin{array}{l} |\phi_{0,0}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ |\phi_{0,1}\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{array}\right\} \quad x = 0$$
$$\left.\begin{array}{l} |\phi_{1,0}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|2\rangle \\ |\phi_{1,1}\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|2\rangle \end{array}\right\} \quad x = 1 \tag{5.3}$$

où x et a sont la base et le bit de l'état $|\phi_{x,a}\rangle$. Ici encore, nous supposons que les pertes et le bruit sont nuls. On définit les bases de mesures

$$\mathcal{B}'_x = \{|\phi_{x,0}\rangle, |\phi_{x,1}\rangle, |2-x\rangle\} \tag{5.4}$$

où $x \in \{0,1\}$. Le protocole d'Ambainis est le suivant :

1. Alice prépare un des quatre états $|\phi_{x,a}\rangle$ où la base x et le bit a sont choisis au hasard. Elle envoie cet état à Bob et il le stocke dans une mémoire quantique.
2. Bob envoie un bit aléatoire b à Alice.
3. Alice révèle la base x et le bit a qu'elle a utilisés.
4. Bob retire l'état de la mémoire et le mesure dans la base $\mathcal{B}'_x$. Soit $\hat{a}$, le résultat de la mesure de Bob.
5. Si $a \neq \hat{a}$, Bob déclare une erreur, traite Alice de tricheuse et fait avorter le protocole.
6. Si le protocole n'a pas avorté, le résultat du pile ou face est $c = x \oplus b$.

Alice ne peut pas utiliser l'attaque EPR pour obtenir avec certitude le résultat c de son choix car les opérateurs densité ρ_0 et ρ_1 générés,

$$\rho_0 = \tfrac{1}{2}|\phi_{0,0}\rangle\langle\phi_{0,0}| + \tfrac{1}{2}|\phi_{0,1}\rangle\langle\phi_{0,1}| = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$
et
$$\rho_1 = \tfrac{1}{2}|\phi_{1,0}\rangle\langle\phi_{1,0}| + \tfrac{1}{2}|\phi_{1,1}\rangle\langle\phi_{1,1}| = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1/2 \end{pmatrix}, \tag{5.5}$$

ne sont pas égaux. Il est assez simple de voir que le biais d'Alice est égal à 0,25 si elle envoie l'état $(2|0\rangle \pm |1\rangle \pm |2\rangle)/\sqrt{6}$ à l'étape 1 et déclare les valeurs de x et de a lui permettant de maximiser sa chance d'obtenir le résultat c voulu tout en minimisant la probabilité de se faire prendre à tricher. La preuve que c'est la triche optimale est non triviale mais a été complétée par A. Ambainis [177]. Comme $\rho_0 \neq \rho_1$, l'attaque EPR est évitée, mais cela permet maintenant à Bob de tricher car il peut mesurer directement l'état reçu avant l'étape 2 et tenter deviner la base x d'Alice. Une stratégie évidente est de mesurer dans la base $\{|0\rangle, |1\rangle, |2\rangle\}$, ce qui lui permet d'obtenir un biais de 0,25. La preuve que cette stratégie est optimale découle directement de la théorie de la mesure de C. W. Helstrom [184]. Une courte revue de cette théorie est présentée à la section 5.5.

Le protocole de R. W. Spekkens et T. Rudolph permettant d'obtenir le même biais de 0,25 est semblable à celui d'Ambainis mais il ne sera pas présenté ici.

5.4 Une vulnérabilité expérimentale

L'analyse de sécurité de A. Ambainis est mathématiquement correcte dans le cas où les pertes et le bruit sont nuls. En pratique, les pertes sont cependant inévitables. En particulier, c'est le cas lorsque les états sont transmis à l'aide photons guidés dans la fibre optique. Il faut également tenir compte des pertes dans la mémoire quantique et du rendement quantique inférieur à 1 des détecteurs. Il est donc indispensable que les protocoles de pile ou face soient capable de tolérer les pertes.

Ainsi, pour tout système réaliste, il est fort probable que le qutrit envoyé par Alice soit perdu en chemin et que Bob n'enregistre rien à l'étape 4, même si Alice et Bob sont tous les deux honnêtes. Que devrait faire Bob dans ce cas ? Il ne peut certainement pas traiter Alice de tricheuse si ses propres détecteurs contribuent significativement à la perte totale du canal ! Deux options évidentes se présentent à Bob [54]. Il peut soit (1) accepter sur parole la base x et le bit a déclarés par Alice soit (2) demander à Alice de recommencer le protocole au complet. Ces deux options sont inacceptables.

Dans le premier cas, si Alice sait que Bob va la croire sur parole s'il ne détecte rien, alors elle peut obtenir le résultat c de son choix avec certitude en n'envoyant tout simplement rien. Ainsi, Bob stocke l'état vide à l'étape 1. (On suppose ici que Bob est incapable de réaliser une mesure non destructive du nombre de photons contenu dans l'impulsion, ce qui lui permettrait en principe de vérifier la présence d'un photon sans perturber son état quantique.) Après avoir reçu le bit b de Bob, Alice est maintenant libre de révéler le x lui permettant d'obtenir le résultat $c = x \oplus b$ de son choix. Bob est assuré de ne rien mesurer à l'étape 4 et, par conséquent, il devra croire Alice sur parole.

Dans le second cas, si Alice et Bob sont d'accord pour recommencer le protocole dans le cas où Bob ne mesure rien, c'est maintenant Bob qui peut obtenir le résultat c de son choix avec certitude en ne faisant presque rien. Lorsque Bob reçoit le qutrit d'Alice, il ne s'en préoccupe tout simplement pas. Il envoie ensuite son bit aléatoire b à Alice. Cette dernière révèle finalement sa base x. Si la valeur de x permet à Bob d'obtenir le résultat c désiré, ce qui survient avec une probabilité de 50%, il prétend que le résultat de sa mesure correspond à l'état révélé par Alice (en réalité, il ne mesure rien du tout). Si, au contraire, la valeur de x ne lui permet pas d'obtenir le résultat c désiré, il n'a qu'à prétendre que le qutrit a été perdu et qu'il faut recommencer. Ceci est répété jusqu'à l'obtention du résultat désiré. Cette stratégie est impossible à détecter par Alice aussitôt que la probabilité p qu'a Bob de détecter le qutrit est de 50% ou moins, pourvu que Bob redemande à Alice de recommencer le protocole avec une probabilité $1 - 2p$, indépendamment du résultat qu'il obtiendrait à l'étape 6.

À moins que Bob soit, à l'étape 1, en mesure de vérifier que l'état envoyé par Alice n'est pas vide (sans toutefois perturber l'état), et parce qu'Alice n'acceptera pas de recommencer le protocole après avoir révélé sa base x et son bit a, Bob n'a qu'une seule possibilité pour se défendre contre l'attaque où Alice envoie un état vide : il doit mesurer le qutrit d'Alice immédiatement après sa réception. S'il n'enregistre rien, il pourra lui demander de recommencer le protocole à partir de zéro jusqu'à ce qu'il enregistre un coup. Autrement dit, il faut réutiliser le canevas du protocole BB84 dans lequel Bob mesure avant qu'Alice ne révèle x et a.

Tel que mentionné dans la section 5.3, cela permettra à une Alice tricheuse de diminuer sa probabilité de se faire prendre à tricher. Cette probabilité est réduite de moitié ou moins, tel que démontré à la section 5.6.2.

Malheureusement, cette modification au protocole d'Ambainis, qui est nécessaire pour tenir compte des pertes, permet maintenant à Bob de briser le protocole. Lorsqu'Alice transmet son qutrit, Bob peut le mesurer dans la base $\{|0\rangle, |1\rangle, |2\rangle\}$. S'il obtient le résultat $|1\rangle$ ou $|2\rangle$, Bob apprend avec certitude la base x d'Alice. Il peut donc choisir le b lui permettant d'obtenir le résultat c désiré. D'autre part, s'il obtient le résultat $|0\rangle$ ou s'il ne détecte rien, il déclare que le qutrit a été perdu en chemin et demande à Alice de recommencer jusqu'à ce qu'il puisse déterminer avec certitude la valeur de x. Au final, le biais de Bob est égal à 0,5 et le protocole est brisé.

Cette faiblesse du protocole d'Ambainis est une conséquence directe de la considération suivante : même si les états ρ_0 et ρ_1 de l'éq. 5.5 ne peuvent être discernés avec certitude à chaque essai, ils peuvent quand même être discernés l'un de l'autre de façon concluante avec une probabilité non nulle. La section suivante présente une courte revue de la notion de mesures concluantes.

5.5 Mesures de Helstrom, concluantes et intermédiaires

Considérons deux mélanges statistiques ρ_0 et ρ_1 arbitraires. Il y a différentes façons de les discerner [185]. Helstrom a étudié les mesures optimales permettant de minimiser la probabilité de deviner incorrectement l'état donné [184]. Supposons que les états ρ_0 et ρ_1 sont équiprobables, la *mesure de Helstrom* permet de deviner correctement l'état avec la probabilité

$$\tfrac{1}{2} + \tfrac{1}{2}\,\mathrm{D}(\rho_0, \rho_1)\,, \tag{5.6}$$

où

$$\mathrm{D}(\rho_0, \rho_1) = \tfrac{1}{2}\,\mathrm{Tr}|\rho_0 - \rho_1| \tag{5.7}$$

est la *distance trace* entre ρ_0 et ρ_1, « Tr » est la trace et $|A| = \sqrt{A^\dagger A}$. En particulier, si A est une matrice diagonale réelle, alors l'élément ij de $|A|$ est égal à la valeur absolue de l'élément ij de A.

Lorsque le *support*[4] de ρ_0 est distinct de celui de ρ_1, une *mesure concluante*[5] existe [186]. On rappelle que ce type de mesure a trois résultats possibles, « 0 », « 1 », et « ? », le dernier étant nommé le *résultat non concluant* [187, 188, 189]. Si le résultat $x \in \{0, 1\}$ est obtenu, alors l'état était ρ_x avec certitude (on suppose que le bruit est nul). De plus, la probabilité d'obtenir un résultat concluant (c'est-à-dire tout sauf « ? ») doit être strictement positive.

Un exemple de mesure concluante pertinent à l'analyse du protocole d'Ambainis en présence de pertes est la mesure dans la base $\{|0\rangle, |1\rangle, |2\rangle\}$, qui permet de discerner entre les états ρ_0 et ρ_1 de l'éq. 5.5 avec une probabilité d'obtenir un résultat concluant égale à 50%. En général, tout protocole de pile ou face quantique qui suit le canevas de BB84 est vulnérable au type d'attaque décrit à la section 5.4 lorsqu'une mesure concluante existe entre les matrices ρ_0 et ρ_1 associées au protocole.

Il faut maintenant se demander si ce genre d'attaque peut s'appliquer même lorsqu'une mesure concluante n'existe pas. La réponse est affirmative. En effet, E. Anderson, S. M. Barnett, A. Chefles, S. Croke, C. R. Gibson et J. Jeffers ont étudié les *mesures quantiques à confiance optimale*[6] (MQCO) qui se situent entre la mesure d'Helstrom et les mesures concluantes [190, 191]. Comme les mesures concluantes, les MQCO ont une probabilité $p < 1$ de produire le résultat non concluant « ? ». Cependant, lorsque le résultat est « 0 » ou « 1 », il est correct avec une probabilité $q > 0$. La mesure d'Helstrom maximise q en fixant $p = 0$, tandis que les mesures concluantes (lorsqu'elles existent) minimisent p en fixant $q = 1$.

4. Le *support* d'une matrice est l'espace généré par l'ensemble de ses vecteurs propres ayant une valeur propre non nulle [186].

5. « Conclusive measurement » ou « unambiguous state discrimination ».

6. « Maximal confidence quantum measurements ».

Il existe donc un compromis entre les deux en ce sens qu'il est parfois possible d'augmenter la probabilité q de deviner correctement l'état au-delà de la borne de Helstrom mais avec le compromis que la probabilité p d'obtenir le résultat non concluant n'est plus nulle.

Pour le pile ou face quantique en présence de pertes, les MQCO sont pertinentes car Bob pourrait tenter de les utiliser pour augmenter son biais au prix d'augmenter aussi sa probabilité de demander à Alice de recommencer le protocole (lorsqu'un résultat non concluant est obtenu) en prétendant avoir perdu l'état quantique. Il est même envisageable qu'il existe une MQCO pour laquelle la probabilité q de deviner correctement l'état est arbitrairement près de 1. Autrement dit, cela permettrait de briser le protocole *de facto*.

Pour démontrer que les MQCO sont pertinentes à l'analyse d'un protocole, considérons le protocole d'Ambainis de la section 5.3 modifié de telle sorte que les états $|\phi_{0,2}\rangle = |2\rangle$ et $|\phi_{1,2}\rangle = |1\rangle$ sont ajoutés. À l'étape 1, Alice choisit au hasard la base $x \in \{0,1\}$ mais le bit $a \in \{0,1,2\}$ est choisi de sorte que $\text{Prob}(a=0) = \text{Prob}(a=1) = 49\%$ tandis que Prob(a=2) = 2%. Le mélange statisique reçu par Bob est donc

$$\rho_0' = \begin{pmatrix} 0.49 & 0 & 0 \\ 0 & 0.49 & 0 \\ 0 & 0 & 0.02 \end{pmatrix} \text{ ou } \rho_1' = \begin{pmatrix} 0.49 & 0 & 0 \\ 0 & 0.02 & 0 \\ 0 & 0 & 0.49 \end{pmatrix}.$$

Ces mélanges statistiques partagent le même support ; ils ne peuvent donc pas être discernés de manière concluante. Néanmoins, une mesure dans la base $\{|0\rangle, |1\rangle, |2\rangle\}$ donne soit $|0\rangle$, ce qui correspond au résultat non concluant « ? », soit $|1\rangle$ ou $|2\rangle$, ce qui est interprété comme ρ_0' ou ρ_1', respectivement. Cette MQCO produit le résultat non concluant avec une probabilité $p = 49\%$. Cependant, lorsque le résultat est concluant, elle permet de deviner correctement l'état avec une probabilité $q = 0.49/0.51 > 96\%$. Ceci est beaucoup mieux que la mesure de Helstrom qui produit toujours une réponse mais qui est correcte avec une probabilité de 73,5% car $\text{D}(\rho_0', \rho_1') = 0.47$. Ainsi, un protocole de pile ou face quantique utilisant ces états permettrait à Bob d'obtenir un biais supérieur à 0,46 pourvu qu'Alice accepte de recommencer le protocole à chaque fois qu'il obtient le résultat non concluant $|0\rangle$.

5.6 Protocole tolérant aux pertes

5.6.1 Description du protocole

Nous présentons maintenant un nouveau protocole de pile ou face quantique et nous prouvons que son biais est égal à 0,4. Contrairement à tous les protocoles précédents, ce biais est indépendant de la valeur des pertes totales du canal entre Alice et Bob. Pour cela, nous

utilisons les états du protocole ATVY [174] combinés avec le canevas du protocole BB84 [3]. Considérons les états

$$\left.\begin{aligned}|\varphi_{0,0}\rangle &= \alpha|0\rangle + \beta|1\rangle \\ |\varphi_{1,0}\rangle &= \alpha|0\rangle - \beta|1\rangle\end{aligned}\right\} \quad a = 0$$
$$\left.\begin{aligned}|\varphi_{0,1}\rangle &= \beta|0\rangle - \alpha|1\rangle \\ |\varphi_{1,1}\rangle &= \beta|0\rangle + \alpha|1\rangle\end{aligned}\right\} \quad a = 1 \tag{5.8}$$

où α et β sont réels et tels que $0 < \beta < \alpha < 1$ et $\alpha^2 + \beta^2 = 1$. On peut donc poser $\alpha = \cos\theta$ et $\beta = \sin\theta$ avec $0 < \theta < 45°$. Ces états sont représentés sur la fig. 5.1 à l'aide de la sphère de Bloch. Comme pour les protocoles précédents, on dit de l'état $|\varphi_{x,a}\rangle$ que x est la base est que a est le bit d'Alice. Nous définissons les bases de mesure de la même façon que nous l'avons fait à l'éq. 5.2 pour les états BB84 :

$$\mathcal{B}''_x = \{|\varphi_{x,0}\rangle, |\varphi_{x,1}\rangle\} \tag{5.9}$$

où $x \in \{0, 1\}$. Les états sont maintenant groupés selon la valeur du bit a et non pas selon la base x tel que c'est le cas pour les protocoles BB84 et d'Ambainis. La raison de ce changement est expliquée plus loin. Voici notre protocole de pile ou face quantique tolérant aux pertes :

1. Alice prépare un des quatre états $|\varphi_{x,a}\rangle$ où la base x et le bit a sont choisis au hasard. Elle envoie cet état à Bob.
2. Bob choisit $\hat{x} \in \{0, 1\}$ au hasard et mesure le qubit reçu dans la base $\mathcal{B}''_{\hat{x}}$. S'il n'enregistre pas de coup, il demande à Alice de recommencer le protocole du début. Autrement, soit $\hat{a}$ le résultat obtenu par Bob.
3. Bob envoie un bit aléatoire b à Alice.

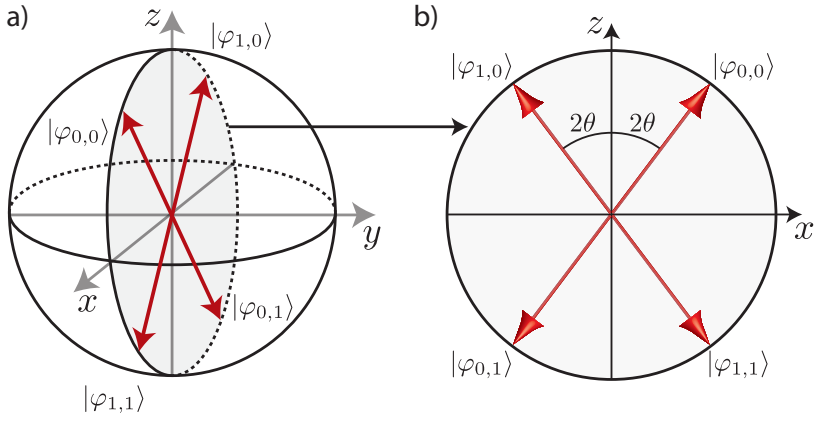

FIGURE 5.1 États $|\varphi_{x,a}\rangle$ représentés sur a) la sphère de Bloch et b) le grand cercle x-z.

4. Alice révèle la base x et le bit a qu'elle a utilisés.
5. Si $x = \hat{x}$ et $a \neq \hat{a}$, Bob déclare une erreur, traite Alice de tricheuse et fait avorter le protocole. Si $x \neq \hat{x}$, Bob n'est pas en mesure de vérifier l'honnêteté d'Alice et le protocole continue.
6. Si le protocole n'a pas avorté, le résultat du pile ou face est $c = a \oplus b$.

Il y a trois différences entre ce protocole et celui de BB84 décrit à la section 5.2 : (1) les états $|\varphi_{x,a}\rangle$ correspondent aux états BB84 $|\psi_{x,a}\rangle$ tournés autour de l'axe y mais sont plus généraux en ce sens que les bases $\mathcal{B}''_x$ ne sont plus nécessairement mutuellement non biaisées [7] ; (2) à l'étape 2, Bob peut demander à Alice de recommencer le protocole dans le cas où il n'enregistre pas de coup ; (3) le résultat du pile ou face est $c = a \oplus b$ au lieu de $c = x \oplus b$.

La première modification simplifie l'analyse du protocole et nous permettra de rendre équilibré tel qu'expliqué à la section 5.6.5. La deuxième est essentielle pour rendre le protocole tolérant aux pertes tel que ce sera expliqué à la section 5.6.3. La troisième modification, qui est la contribution originale du protocole ATVY, rend distincts les mélanges statistiques ϱ_0 et ϱ_1 générés par Alice pour dissimuler le bit $a = 0$ ou $a = 1$ à l'étape 1. On calcule que

$$\begin{aligned} \varrho_0 &= \tfrac{1}{2}|\varphi_{0,0}\rangle\langle\varphi_{0,0}| + \tfrac{1}{2}|\varphi_{1,0}\rangle\langle\varphi_{1,0}| = \begin{pmatrix} \alpha^2 & 0 \\ 0 & \beta^2 \end{pmatrix} \\ &\text{et} \\ \varrho_1 &= \tfrac{1}{2}|\varphi_{0,1}\rangle\langle\varphi_{0,1}| + \tfrac{1}{2}|\varphi_{1,1}\rangle\langle\varphi_{1,1}| = \begin{pmatrix} \beta^2 & 0 \\ 0 & \alpha^2 \end{pmatrix}. \end{aligned} \tag{5.10}$$

La différence entre le protocole BB84 et ce nouveau protocole est minime mais les conséquences sont énormes. En effet, lorsque le résultat du pile ou face est calculé avec la base x d'Alice, le protocole est complètement brisé en raison de l'attaque EPR. Lorsqu'il est calculé avec le bit a d'Alice, le protocole est non seulement sécuritaire mais il est également tolérant aux pertes.

De plus, nous verrons à la section 5.6.3 que, contrairement aux mélanges statistiques ρ_0 et ρ_1 du protocole d'Ambainis (cf. éq. 5.5), les états ϱ_0 et ϱ_1 ne peuvent pas être discernés de façon concluante ou avec une mesure quantique à confiance optimale (MQCO). Autrement dit, la triche optimale de Bob nécessite une mesure de Helstrom, ce qui est la clé de la tolérance aux pertes.

Nous avons présenté notre protocole comme une modification du protocole de BB84. Il est également utile de le comparer au protocole ATVY. La différence entre celui-ci est le nôtre est que le canevas ATVY est tel que Bob stocke l'état envoyé par Alice à l'étape 1 et

7. « Mutually unbiased ».

retarde la mesure jusqu'à ce qu'Alice ait révélé sa base x et son bit a. Ceci avait pour but de rendre la triche d'Alice plus difficile car Bob peut mesurer l'état dans la bonne base $\mathcal{B}''_{\hat{x}}$. Malheureusement, la conséquence est que le protocole n'est pas tolérant aux pertes tel que nous l'avons expliqué ci-haut.

Dans la section suivante, nous montrons que les biais d'Alice et Bob sont

$$\varepsilon_A = (1 + 2\alpha\beta)/4 \quad \text{et} \quad \varepsilon_B = \alpha^2 - 1/2\,,$$

respectivement, où $\alpha = \cos\theta$ et $\beta = \sin\theta$, et nous présentons des stratégies de triche pour obtenir ces biais. On montre également que le choix de l'angle θ permet de faire varier ces biais et, entre autre, d'obtenir un protocole équilibré ayant un biais de 0,4.

5.6.2 Triche optimale d'Alice

Il serait relativement simple de déterminer la triche optimale d'Alice si elle n'envoyait que des états purs à la première étape du protocole. Cependant, l'analyse du protocole BB84 [3] a montré qu'il faut également tenir compte de la possibilité qu'Alice envoie la moitié d'une paire intriquée à Bob. Tenir compte de toutes les possibilités est ardu. Heureusement, l'analyse de notre protocole bénéficie grandement de l'analyse du protocole ATVY que R. W. Spekkens et T. Rudolph ont déjà faite [175].

Nous débutons notre analyse en supposant d'abord que Bob retarde sa mesure jusqu'à ce qu'Alice ait révélé sa base x et son bit a. Comme nous l'avons déjà mentionné, ceci nous donne le protocole ATVY. Il découle directement de l'analyse de R. W. Spekkens et T. Rudolph que la triche optimale d'Alice lui donne un biais

$$\varepsilon'_A \leq \frac{\sin 2\theta}{2} = \sin\theta\cos\theta = \alpha\beta\,. \tag{5.11}$$

Pour analyser notre protocole, il faut tenir compte du fait que Bob mesure avant qu'elle ne révèle l'état qu'elle a envoyé. Cette différence rend la triche d'Alice plus efficace (cela augmente son biais) parce que la mesure de Bob ne peut être ajustée pour maximiser sa probabilité de discerner entre l'état qu'elle prétend avoir envoyé et celui qu'elle a réellement envoyé.

On rappelle qu'à l'étape 3 de notre protocole, Bob envoie un bit aléatoire b qui doit être choisi indépendamment du choix de sa base de mesure $\hat{x}$ et du résultat $\hat{a}$ de sa mesure. Ceci est crucial car cela empêche Alice d'obtenir de l'information sur la mesure de Bob. Il s'en suit que la base x et le bit a qu'elle révèle à l'étape 4 ne peuvent pas dépendre de la mesure de Bob. En particulier, on aura $\hat{x} = x$ avec une probabilité de 50% car $\hat{x}$ est choisi au hasard

lorsque Bob est honnête. Si tel est le cas, la mesure de Bob est identique à celle qu'il aurait faite dans le protocole ATVY. Cela implique que la stratégie de triche d'Alice contre notre protocole se traduit en une stratégie identique contre le protocole ATVY car il n'y a aucune différence entre le cas où Bob mesure avant ou après qu'Alice ait révélé le x et a et de son choix. Considérons maintenant une stratégie quelconque d'Alice lui permettant d'obtenir un biais ε_A (ε'_A) contre notre protocole (contre le protocole AVTY).

Considérons une exécution de notre protocole dans laquelle Alice utilise cette stratégie de triche. Avec une probabilité de 50%, Bob choisit la même base de mesure qu'il aurait utilisée dans le protocole ATVY, auquel cas Alice obtient le résultat désiré avec une probabilité $\frac{1}{2} + \varepsilon'_A$. Avec la probabilité complémentaire de 50%, Bob ne peut vérifier l'honnêteté d'Alice et elle obtient le résultat désiré avec une probabilité d'au plus 1. Au total, la probabilité qu'Alice obtienne le résultat désiré est

$$\tfrac{1}{2} + \varepsilon_A \leq \tfrac{1}{2}\left(\tfrac{1}{2} + \varepsilon'_A\right) + \tfrac{1}{2} \times 1 = \tfrac{3}{4} + \tfrac{1}{2}\varepsilon'_A \,.$$

Il s'en suit que

$$\varepsilon_A \leq \frac{1 + 2\varepsilon'_A}{4} \leq \frac{1 + 2\alpha\beta}{4} \,, \tag{5.12}$$

où la dernière inégalité découle de l'éq. 5.11.

Nous montrons maintenant comment Alice peut atteindre cette borne. La triche optimale d'Alice ne nécessite pas d'intrication. En fait, il lui suffit d'envoyer au hasard l'état $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ou l'état $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Supposons qu'elle a envoyé l'état $|+\rangle$ (l'autre cas est similaire) et reçu le bit b de Bob à l'étape 3. Si son résultat désiré est c, elle choisit $a = c \oplus b$ et prétend qu'à l'étape 4, elle a envoyé l'état $|\varphi_{a,a}\rangle$. Avec une probabilité de 50%, Bob avait déjà choisi $\hat{x} \neq a$, auquel cas il ne peut attraper Alice à tricher. Avec la probabilité complémentaire, il a choisi $\hat{x} = a$, auquel cas Alice évite de se faire prendre à tricher avec une probabilité

$$|\langle +|\varphi_{a,a}\rangle|^2 = \left(\tfrac{1}{\sqrt{2}}\alpha + \tfrac{1}{\sqrt{2}}\beta\right)^2 = \frac{(\alpha+\beta)^2}{2} = \tfrac{1}{2} + \alpha\beta \,,$$

où la dernière égalité découle de $\alpha^2 + \beta^2 = 1$. En combinant toutes les possibilités, Alice obtient le résultat désiré avec une probabilité

$$\frac{1}{2} + \frac{1}{2}\left(\frac{1}{2} + \alpha\beta\right) = \frac{3 + 2\alpha\beta}{4}$$

et son biais est

$$\varepsilon_A = \frac{3 + 2\alpha\beta}{4} - \frac{1}{2} = \frac{1 + 2\alpha\beta}{4} \,, \tag{5.13}$$

ce qui permet d'atteindre la borne supérieure de l'éq. 5.12.

On remarque que l'état $|+\rangle$ est situé exactement à mi-chemin entre $|\varphi_{0,0}\rangle$ et $|\varphi_{1,1}\rangle$, tel qu'illustré sur la fig. 5.2. Il est donc positionné de façon à donner toute la latitude possible à Alice pour révéler le bit a lui permettant d'obtenir le résultat désiré à l'étape 4. Parallèlement, il minimise également la probabilité qu'elle se fasse prendre à tricher. Le même raisonnement s'applique à l'état $|-\rangle$.

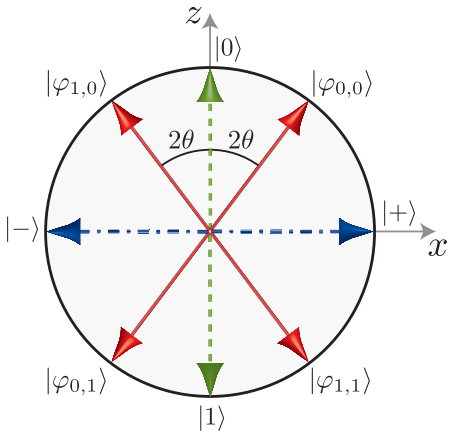

FIGURE 5.2 États $|\varphi_{x,a}\rangle$ représentés sur le grand cercle x-z, états $|+\rangle$ et $|-\rangle$ correspondant aux états de la triche optimale d'Alice et états $|0\rangle$ et $|1\rangle$ définissant la base de mesure de la triche optimale de Bob.

5.6.3 Triche optimale de Bob

L'approche traditionnelle permettant de déterminer le biais de Bob dans un jeu de pile ou face quantique donné consiste à utiliser les éq. 5.6 et 5.7 pour calculer la distance trace et ainsi obtenir la probabilité que la mesure d'Helstrom permette à Bob de deviner correctement le bit a d'Alice. Pour notre protocole, on trouve que $\mathrm{D}(\varrho_0, \varrho_1) = \alpha^2 - \beta^2 = 2\alpha^2 - 1$. La probabilité associée est $\frac{1}{2} + \frac{1}{2}\mathrm{D}(\varrho_0, \varrho_1) = \alpha^2$. Avec cette analyse, on conclut que le biais maximal de Bob est

$$\varepsilon_B = \alpha^2 - 1/2. \tag{5.14}$$

Cependant, comme nous l'avons vu, cette approche n'est pas appropriée dans le contexte ou les pertes sont non nulles car elle ne tient pas compte de la possibilité que Bob augmente son biais en exploitant une mesure concluante ou une mesure quantique à confiance maximale. Fort heureusement, l'analyse de la triche optimale de Bob est évidente pour notre protocole. Pour les deux valeurs possibles de $a \in \{0, 1\}$ qu'Alice a pu choisir à l'étape 1, l'éq. 5.10 nous montre les mélanges statistiques ϱ_a qu'elle génère. Mathématiquement, on remarque que

$\varrho_0 = \alpha^2|0\rangle\langle 0| + \beta^2|1\rangle\langle 1|$ et $\varrho_1 = \beta^2|0\rangle\langle 0| + \alpha^2|1\rangle\langle 1|$. Du point de vue d'un Bob tricheur, qui ne cherche qu'à deviner la valeur de a du mieux qu'il peut en ayant la liberté de demander à Alice de recommencer s'il croit que cela peut augmenter ses chances de deviner a correctement, cette situation est strictement équivalente au scénario où Alice aurait envoyé l'état $|0\rangle$ avec une probabilité α^2 ou l'état $|1\rangle$ avec une probabilité β^2 lorsque $a = 0$, et vice versa dans le cas où $a = 1$.

Ainsi, cette situation est purement classique car les états envoyés dans le scénario équivalent peuvent être associés à des états classiques orthogonaux. Ainsi, Bob obtient toute l'information possible sur le bit a d'Alice en mesurant dans la base $\{|0\rangle, |1\rangle\}$, ce qui constitue sa triche optimale. Cette mesure correspond à la mesure de Helstrom. En particulier, le résultat de cette mesure n'indique nullement à Bob s'il obtiendrait un avantage à demander à Alice de recommencer le protocole du début.

En résumé, la stratégie optimale de Bob consiste à mesurer le qubit d'Alice dans la base $\{|0\rangle, |1\rangle\}$ dans le but de deviner correctement la valeur de a avec une probabilité de succès de α^2 et une probabilité d'insuccès de $\beta^2 = 1 - \alpha^2$, ce qui correspond au biais donné à l'éq. 5.14. Encore une fois, cela n'est pas trop surprenant car l'état $|0\rangle$ ($|1\rangle$) est situé exactement à mi-chemin entre les états $|\varphi_{0,0}\rangle$ et $|\varphi_{1,0}\rangle$ ($|\varphi_{0,1}\rangle$ et $|\varphi_{1,1}\rangle$) correspondants au bit $a = 0$ ($a = 1$), tel qu'illustré sur la fig. 5.2.

5.6.4 Biais correspondants aux états BB84

Il est intéressant d'analyser la sécurité de notre protocole lorsqu'Alice et Bob utilisent les états BB84. Ceci est le cas lorsque $\theta = 22{,}5°$. Les états $|\varphi_{x,a}\rangle$ (éq. 5.8) sont alors équivalents aux états BB84 (éq. 5.1) tournés de 45° autour de l'axe y. Les biais d'Alice et de Bob sont obtenus à l'aide des éq. 5.13 et 5.14 :

$$\varepsilon_A = \frac{2+\sqrt{2}}{8} \approx 0{,}427 \tag{5.15}$$

$$\varepsilon_B = \frac{\sqrt{2}}{4} \approx 0{,}354. \tag{5.16}$$

Les probabilités P_A et P_B qu'Alice et Bob obtiennent le résultat de leur choix en trichant de façon optimale (en supposant toujours que l'autre joueur et honnête) sont donc

$$P_A = \frac{1}{2} + \varepsilon_A = \frac{6+\sqrt{2}}{8} \approx 92{,}7\% \tag{5.17}$$

$$P_B = \frac{1}{2} + \varepsilon_B = \frac{2+\sqrt{2}}{4} \approx 85{,}4\%\,. \tag{5.18}$$

Finalement, la probabilité maximale qu'Alice se fasse prendre à tricher par Bob est

$$P_A^* = 1 - P_A \approx 7{,}3\% \,. \tag{5.19}$$

Les biais ne sont pas équilibrés. Ceci est une conséquence directe du fait que la mesure de Bob doit avoir lieu avant qu'Alice ne révèle sa base de préparation, tel qu'expliqué à la section 5.6.2.

5.6.5 Protocole équilibré

Dans cette section, nous trouvons la valeur de α permettant d'obtenir le même biais pour Alice et Bob. Nous avons simplement besoin de remplir la condition

$$\varepsilon_A = \varepsilon_B \,.$$

Pour notre protocole, cela donne

$$\frac{1 + 2\alpha\beta}{4} = \alpha^2 - \frac{1}{2} \,,$$

sous la condition que $\alpha^2 + \beta^2 = 1$. La solution de cette équation est

$$\alpha = \sqrt{0{,}9} \;\text{ et }\; \beta = \sqrt{0{,}1} \,,$$

et donc $\theta \approx 18{,}4°$. Ces valeurs donnent

$$\varepsilon_A = \varepsilon_B = 0{,}4 \,, \tag{5.20}$$

ce qui définit un protocole équilibré tolérant aux pertes ayant un biais 0,4. La probabilité équivalente que le tricheur obtienne le résultat désiré avec la triche optimale est donc

$$P_A = P_B = 90\% \tag{5.21}$$

pourvu bien sûr qu'il n'y ait qu'un seul tricheur. La probabilité maximale qu'Alice se fasse prendre à tricher est donc $P_A^* = 10\%$.

5.6.6 Canal fantôme

Comme nous venons de le montrer, notre protocole est tolérant aux pertes. Malgré cela, cette tolérance aux pertes peut disparaître si certains détails de son implémentation sont

négligés. Un *canal fantôme*[8] est défini comme une source d'information sur l'état d'Alice qui n'est pas incluse dans sa description $|\varphi_{x,a}\rangle$ et que Bob peut exploiter pour augmenter sa probabilité d'obtenir le résultat désiré. Par exemple, notre protocole serait complètement brisé si les états quantiques $|\varphi_{x,a}\rangle$ générés à l'aide de photons avaient chacun une longueur d'onde distincte des trois autres. Les canaux fantômes ont été étudiés en profondeur dans le contexte de la DQC.

Un exemple important de canal fantôme surviendrait si notre protocole de pile ou face quantique était basé sur l'utilisation d'une source laser atténuée pour générer les états d'Alice, tel que c'est souvent le cas pour la DQC. Ce problème émerge du fait qu'il devient possible de discerner les mélanges statistiques ϱ_0 and ϱ_1 (éq. 5.10) de façon concluante lorsque l'impulsion laser contient deux photons ou plus préparés dans le même état. Pour réaliser ceci, il suffit que Bob mesure un des deux photons dans la base $\mathcal{B}_0''$ et l'autre dans la base $\mathcal{B}_1''$ (éq. 5.9). Si les deux mesures produisent le même résultat, il correspond nécessairement au bit a d'Alice car au moins une des deux mesures a été faite dans la bonne base. Ceci survient avec une probabilité $(\alpha^2 - \beta^2)^2$ dans le cas idéal. Avec les états équilibrés, la probabilité que Bob obtienne le résultat concluant est donc égale à 64% chaque fois que l'impulsion contient deux photons, ce qui implique que cette implémentation est complètement brisée car Bob peut demander à Alice de recommencer jusqu'à l'obtention du résultat concluant (pourvu bien sûr qu'Alice accepte de recommencer autant de fois que Bob le demande).

Une solution à ce problème est d'utiliser l'intrication pour générer les photons, tel que discuté à la section 5.11.2.

5.7 Résumé du protocole et questions ouvertes

La primitive du pile ou face quantique a fait l'objet de nombreuses études. Plusieurs approches ont été envisagées depuis les tout débuts de la cryptographie quantique. Cependant, en présence de pertes sur le canal entre les joueurs, tous les protocoles précédents sont soit *complètement brisés* [174, 177, 176, 175, 178], soit *brisés de facto* [180]. Nous avons présenté le premier protocole de pile ou face quantique tolérant aux pertes, ce qui signifie que le biais du protocole est indépendant de la grandeur de ces pertes. Nous avons prouvé que notre protocole peut être équilibré de sorte que le biais d'Alice et de Bob est égal à 0,4, ce qui implique qu'un tricheur peut obtenir le résultat désiré avec une probabilité d'au plus 90% (en supposant qu'un seul joueur triche). Nous avons également explicité les triches optimales d'Alice et de Bob.

Une question ouverte importante émerge de notre analyse : quel est le plus petit biais

8. « Side channel ».

possible d'un protocole tolérant aux pertes ? Autrement dit, est-ce que le biais de 0,4 de notre protocole est optimal ou bien existe-t-il un protocole avec un biais inférieur ?

Finalement, il est important de mentionner à ce point que notre protocole fait partie de la catégorie des *protocoles de pile ou face forts*[9] pour lesquels le biais est indépendant du résultat désiré par chaque joueur. Il existe une autre catégorie de protocoles de pile ou face quantiques pour lesquels le résultat désiré par Alice est connu de tous et est distinct de celui désiré par Bob. Par exemple, si le pile ou face est utilisé pour déterminer qui d'Alice ou Bob remportera un prix alléchant (on suppose que les deux joueurs désirent gagner ce prix), et que le résultat $c = 0$ ($c = 1$) signifie qu'Alice (Bob) gagne, alors il est évident que si Alice (Bob) triche, elle (il) essaiera d'obtenir le résultat $c = 0$ ($c = 1$). Ce type de protocole se nomme *protocole de pile ou face faible.*[10] Ces protocoles ne sont pas contraints par la borne de Kitaev [53] et peuvent en principe avoir un biais arbitrairement près de 0 [192]. Il est donc naturel de se demander si un protocole de pile ou face quantique tolérant aux pertes dont le biais est inférieur à la borne de Kitaev ou encore arbitrairement près de 0 existe. Nous savons déjà que le protocole de R. W. Spekkens et T. Rudolph [193] ainsi que celui de C. Mochon [192] sont complètement brisés en présence de pertes. Est-ce que ces protocoles peuvent être modifiés ou reformulés pour être tolérant aux pertes ?

5.8 Pile ou face en présence de bruit

Notre protocole est tolérant aux pertes mais il n'est malheureusement pas tolérant au bruit causé par les imperfections du montage [54]. Le bruit est causé par toute imperfection dans la préparation, la transmission et la mesure des états et résulte parfois en l'obtention d'un résultat non conforme avec ce qui est attendu dans le cas idéal. Les coups sombres des détecteurs sont un exemple de source de bruit. La conséquence du bruit est qu'il est possible que Bob enregistre une erreur à l'étape 5 de notre protocole même lorsque les deux joueurs sont totalement honnêtes. Dans le cas idéal, une erreur implique nécessairement qu'Alice triche, mais ce n'est plus le cas lorsque cette erreur peut être causée par le bruit. Ainsi, Bob ne peut traiter Alice de tricheuse en toute légitimité lorsqu'il obtient une erreur. Pire encore, Bob peut maintenant prétendre qu'il a enregistré une erreur lorsque le résultat du pile ou face ne correspond pas à ce qu'il désire. Si Alice et Bob recommencent à chaque fois que Bob obtient une erreur, Bob peut briser le protocole en demandant à Alice de recommencer jusqu'à l'obtention du résultat désiré en ne mesurant rien du tout. Si la primitive du pile ou face est problématique en présence de bruit, existe-t-il une autre tâche intéressante et utile

9. « Strong coin flipping ».
10. « Weak quantum coin flipping ».

que l'on peut accomplir à l'aide de ce protocole ? Nous croyons que la réponse est affirmative, tel que discuté à la section 5.9.

5.9 Pile ou face séquentiel

Comme que nous venons de le voir, l'implémentation d'un protocole de pile ou face quantique en présence de bruit semble très problématique. Malgré cela, existe-t-il une tâche différente pouvant tirer profit du fait que le présence d'un tricheur augmente la probabilité d'erreur ?

Pour rendre les choses plus précises, définissons une *exécution* du protocole comme une application du protocole se terminant soit en l'obtention d'un résultat $c = 0$ ou $c = 1$, soit en une erreur déclarée par Bob. Lorsqu'Alice et Bob sont honnêtes, on définit P_0 (P_1) comme la probabilité qu'une exécution se termine avec $c = 0$ ($c = 1$) et P^* comme la probabilité que l'exécution se termine avec une erreur. On a

$$P_0 + P_1 + P^* = 1 \qquad \text{(cas honnête)}. \tag{5.22}$$

La probabilité P^* correspond donc à la probabilité d'erreur intrinsèque du montage. On suppose que ce taux d'erreur intrinsèque est indépendant de toute action (potentiellement malveillante) entreprise par Alice et Bob.

Lorsqu'Alice triche, elle déclare le bit a lui permettant d'obtenir le résultat désiré. Ainsi, les résultats possibles sont soit qu'elle obtient le résultat désiré avec une probabilité P_A, soit que Bob (qui est honnête) déclare une erreur avec une probabilité $P_A^* = 1 - P_A$. Les erreurs sont provoquées soit par le bruit du montage, soit par la triche d'Alice, d'où

$$P_A^* = P^* + (1 - P^*)\left(\tfrac{1}{2} - \varepsilon_A\right) \geq \left(\tfrac{1}{2} - \varepsilon_A\right). \tag{5.23}$$

La dernière inégalité est obtenue lorsque $P^* = 0$. Ainsi,

$$P_A = 1 - P_A^* = (1 - P^*)\left(\tfrac{1}{2} - \varepsilon_A\right) \leq \tfrac{1}{2} + \varepsilon_A \tag{5.24}$$

tel qu'attendu.

De la même façon, on suppose que Bob déclare toujours une erreur lorsque le résultat ne le satisfait pas. Ainsi, les résultats possibles lorsque Bob triche (et qu'Alice est honnête) sont soit que Bob obtient le résultat désiré avec une probabilité P_B, soit qu'il déclare une erreur avec une probabilité $P_B^* = 1 - P_B$. On obtient ainsi les mêmes équations que pour Alice en remplaçant P_A, P_A^* et ε_A par P_B, P_B^* et ε_B.

Notre protocole est donc *sensible à la présence d'un tricheur*[11] car $P_A^* > P^*$ et $P_B^* > P^*$ pour toute valeur ε_A et ε_B inférieure à $\frac{1}{2}$. Sur une seule exécution du protocole, cette propriété n'est malheureusement pas vraiment utile car les fluctuations statistiques sont telles qu'*a priori*, l'obtention d'une erreur ne permet pas à de conclure avec certitude qu'un des deux joueurs triche (à moins que P^* soit pratiquement négligeable). Cependant, une application répétée du protocole où le tricheur triche sur chaque exécution le forcera à révéler sa présence *a posteriori* via l'augmentation du taux d'erreur. Dans la limite asymptotique, le taux d'erreur indique le nombre d'exécutions dont le résultat est complètement biaisé. Par exemple, si Alice triche, Bob conclut qu'elle a réussi à choisir tous les bits aussitôt que $P_A^* \geq \frac{1}{2} - \varepsilon_A$ (Bob ne prend aucune chance et suppose qu'une Alice tricheuse peut réduire P^* à 0). Si Alice triche de façon non optimale ou encore triche seulement sur une fraction des exécutions, Alice aura choisi le résultat d'une fraction $P_A^* / \left(\frac{1}{2} - \varepsilon_A\right)$ des exécutions ayant produit un bit. Le cas où Bob triche est similaire. Lorsque les deux joueurs sont honnêtes, un taux d'erreur non nul doit quand même être interprété par Alice comme si Bob triche et elle supposera qu'il a réussi à choisir à sa guise une fraction $P^* / \left(\frac{1}{2} - \varepsilon_B\right)$ des exécutions ayant produit un bit. De la même façon, Bob supposera que Alice a réussi à choisir une fraction $P^* / \left(\frac{1}{2} - \varepsilon_A\right)$ des exécutions ayant produit un bit. Ceci illustre l'importance de minimiser le taux d'erreur intrinsèque du montage.

On remarque que ces conclusions ne sont valides que si Alice et Bob utilisent un protocole tolérant aux pertes car autrement le tricheur pourrait exploiter les pertes pour augmenter son biais au lieu d'avoir recours à une stratégie qui augmente la probabilité d'erreur.

Ainsi, une application répétée d'un protocole de pile ou face quantique tolérant aux pertes force le tricheur à révéler sa présence. Existe-t-il une tâche impossible à réaliser classiquement permettant de tirer profit de cet avantage ? La tâche de *génération d'une chaîne de bits aléatoires* a été considérée par J. Barrett et S. Massar [54]. L'objectif est de générer une chaîne de bits de longueur prédéterminée et dont l'entropie est au-delà d'une certaine valeur (idéalement, on voudrait que l'entropie d'une chaîne de n bits soit égale à n). Or, il a été prouvé récemment que cette tâche est réalisable classiquement [179], ce qui rend une approche quantique beaucoup moins intéressante.

La tâche que nous considérons, que nous nommons *pile ou face séquentiel*, est légèrement différente. Supposons qu'Alice et Bob ont besoin de tirer à pile ou face un nombre indéterminé de fois et que chaque joueur a la possibilité d'arrêter de jouer à n'importe quel moment et pour n'importe quelle raison, incluant la possibilité qu'il a perdu confiance en l'autre joueur. Ce scénario serait potentiellement utile dans le contexte d'un casino en ligne. En effet, il très plausible que la maison (Alice) et le joueur (Bob) ne se fassent pas confiance mais qu'ils

11. « Cheat sensitive ».

désirent quand même jouer pour une durée indéfinie. Cette tâche peut être accomplie par une application répétée de notre protocole de pile ou face quantique tolérant aux pertes. Tel que mentionné ci-haut, le bénéfice est que si le joueur ou la maison triche, cela se reflétera sur le taux d'erreur obtenu. Si les deux désirent jouer indéfiniment, ils devront s'efforcer de ne pas tricher car autrement quelqu'un arrêtera éventuellement de jouer par perte de confiance. Comme le taux d'erreur n'est jamais nul, la maison (le joueur) peut secrètement déterminer le taux d'erreur maximal qu'elle (qu'il) tolérera avant même de commencer à jouer, mais elle (il) devrait également tolérer un taux d'erreur P^* minimal égal au taux d'erreur intrinsèque au montage. On note que la génération d'une chaîne de bit ne peut pas être utilisée dans ce contexte. En effet, l'utilisation séquentielle de chaque bit de cette chaîne (qui est générée d'un seul coup) dans un contexte de jeu de hasard serait telle que le joueur et la maison pourraient déterminer à l'avance qui remporterait chaque mise et pourrait donc arrêter de jouer dès le que la situation serait défavorable.

Nous croyons que le pile ou face séquentiel est classiquement impossible à réaliser de façon inconditionnellement sécuritaire pour la simple raison que chaque exécution doit être réalisée d'une manière indépendante de toutes les autres et la séquence doit être ordonnée dans le temps. Ainsi, chaque éxécution doit produire le résultat $c = 0$, $c = 1$ ou une erreur, et chaque résultat ne doit pas faire partie d'une séquence générée à l'avance comme c'est le cas pour la génération d'une chaîne de bits. Autrement dit, chaque éxécution doit nécessairement être le résultat d'un pile ou face. Comme chaque pile ou face est classiquement brisé, alors chaque éxécution de la séquence générée peut être complètement biaisée par un tricheur. Ces arguments semblent supporter notre hypothèse, mais au moment d'écrire cette thèse, elle n'a pas été prouvée formellement.

Une étude plus poussée de cette question est nécessaire. En particulier, une analyse de la sécurité du protocole de pile ou face séquentiel dans le cas où l'ensemble statistique est de taille finie est requise.

5.10 Expériences antérieures

Le pile ou face quantique a fait l'objet de deux expériences antérieures à celle de cette thèse. La première, réalisée par G. Molina-Terriza, A. Vaziri, R. Ursin et A. Zeilinger et publiée en 2005, est une implémentation du protocole d'Ambainis [194]. Pour préparer les qutrits nécessaires, ils ont tiré profit du fait que le moment angulaire orbital photonique possède une infinité de modes propres. En se restreignant à trois, ils ont réalisé une source de paires de qutrits intriqués. Ainsi, Alice préparait le qutrit à envoyer à Bob en mesurant l'autre qutrit. Malgré cette avancée technologique, il reste que le protocole d'Ambainis est

complètement brisé en présence de pertes, indépendamment du fait que le bruit est nul ou pas. Par conséquent, toute implémentation basée sur ce protocole est également complètement brisée. Ceci serait également le cas de toute implémentation du pile ou face séquentiel basée sur le protocole d'Ambainis.

La deuxième implémentation, réalisée par A. T. Nguyen, J. Frison, K. Phan Huy et S. Massar, a été publiée en 2008 [180]. Tel que mentionné dans l'introduction de ce chapitre, ils ont proposé un protocole dont l'implémentation n'est pas complètement brisée en présence de pertes (c'est-à-dire que le biais est inférieur à 0,5) si on exclut la possibilité que Bob exploite le bruit pour briser le protocole. Pour obtenir ce résultat, le protocole est tel que Bob doit toujours répondre même s'il ne détecte rien. Cela semblerait très étrange si le protocole suivait le canevas de BB84 ou celui de ATVY car Alice pourrait alors briser le protocole en n'envoyant rien du tout. Or, ce n'est pas le cas car l'implémentation du protocole est telle que Bob peut facilement contourner cette attaque. Il serait hors propos de décrire ce protocole et son implémentation et nous dirigeons le lecteur vers l'article pour tous les détails [180]. Nous nous contenterons de mentionner ses inconvénients qui, selon nous, limitent grandement son utilité.

Nous avons déjà mentionné que le biais de ce protocole est inférieur à 0,5 malgré la présence de pertes sur le canal. Il est cependant crucial de rappeler que ce biais augmente de façon exponentielle en fonction de la perte totale du canal entre Alice et Bob (ceci inclut toutes les pertes optiques et le rendement des détecteurs). Plus précisément, l'analyse du protocole montre que le biais d'Alice est

$$\varepsilon = \tfrac{1}{2} \exp\left[-\eta_T \left(1 - 2\sqrt{q}\right) \alpha^2\right], \tag{5.25}$$

où η_T est la transmittance du canal, q est le taux d'erreur intrinsèque et α^2 est un facteur relié à la puissance de l'impulsion cohérente utilisée. En guise d'exemple, on calcule que pour une transmission parfaite, c'est-à-dire $\eta_T = 1$ et $q = 0$, on peut ajuster α^2 de sorte que le protocole est équilibré et on a $\varepsilon \approx 0{,}39$. Cette situation est cependant irréaliste. En pratique, on a typiquement que $\eta_T \leq 0{,}1$, et donc que $\varepsilon \geq 0{,}472$. L'expérience réalisée par Nguyen *et al.* était telle que les pertes provenaient principalement des détecteurs. Autrement dit, la perte de la fibre optique reliant Alice et Bob était pratiquement nulle. Malgré cette situation avantageuse, le biais obtenu est de 0,4971 et le tricheur (Alice en l'occurrence) pouvait obtenir le résultat de son choix avec une probabilité de 99,71%. On note également que cela ouvre la porte à la possibilité qu'Alice gonfle artificiellement les pertes du canal dans le but d'augmenter son biais encore plus près de 0,5 sans même augmenter la probabilité qu'elle se fasse prendre à tricher. En effet, l'éq. 5.25 montre clairement que $\varepsilon \to 0{,}5$ lorsque

$\eta_T \to 0$. Comme Bob est physiquement incapable de déterminer si les pertes du canal ont été gonflées artificiellement ou pas, il est à la merci de cette attaque. Pour cette raison, ce protocole est brisé *de facto*. Tous ces inconvénients limitent donc sévèrement l'utilité de ce protocole et de son implémentation pour réaliser une expérience de pile ou face quantique ou même de pile ou face séquentiel.

Tout comme notre protocole dans le contexte d'une seule exécution, celui de NFPM n'est pas tolérant au bruit et son biais est en réalité égal à 0,5.

5.11 Pile ou face séquentiel expérimental

La source d'intrication temporelle que nous avons présentée au chapitre 4 peut être utilisée directement dans l'implémentation de la tâche de pile ou face séquentiel. Le reste de ce chapitre est consacré à la description de cette expérience.

5.11.1 Source d'intrication

Considérons la source d'intrication temporelle de la fig. 4.9 décrite à la section 4.4 (page 83). Cette source crée des paires de qubits photoniques dans l'état

$$\tfrac{1}{\sqrt{2}}(|t_0, t_0\rangle + |t_1, t_1\rangle). \tag{5.26}$$

Le premier qubit (centré à 811,7 nm) est donné à Alice afin qu'elle le mesure à l'aide de son analyseur temporel universel (ATU) à l'air libre (cf. section 4.4.1). Pour les besoins de cette expérience, la lame quart d'onde Q3 (cf. fig. 4.7, p. 80) a été enlevée. Supposons pour l'instant que la phase relative ϕ_A entre les bras de l'interféromètre de l'ATU est nulle. Cet ATU est tel que chaque détection survient dans la fenêtre temporelle f_2 avec une probabilité de 50%. Dans cette fenêtre, la base de mesure sélectionnée par la lame demi-onde D2 combinée avec le cube polariseur C2 est

$$\{\cos\theta_A|t_0\rangle + \sin\theta_A|t_1\rangle, \sin\theta_A|t_0\rangle - \cos\theta_A|t_1\rangle\}. \tag{5.27}$$

Autrement, chaque détection survient dans la fenêtre f_0 avec une probabilité de 25%, ce qui correspond à une projection sur l'état $|t_0\rangle$, ou dans la fenêtre f_1 avec une probabilité de 25%, ce qui correspond à une projection sur $|t_1\rangle$.

Comme les deux qubits sont préparés dans l'état $\frac{1}{\sqrt{2}}(|t_0, t_0\rangle + |t_1, t_1\rangle)$, le fait de projeter le qubit d'Alice sur $\cos\theta_A|t_0\rangle + \sin\theta_A|t_1\rangle$, ce qui survient avec une probabilité de 25%, a pour effet de préparer le qubit de Bob dans le même état. Le même raisonnement permet de

montrer que la mesure d'Alice préparera le qubit de Bob dans l'état $\sin\theta_A|t_0\rangle - \cos\theta_A|t_1\rangle$, $|t_0\rangle$ ou $|t_1\rangle$, chacun avec une probabilité de 25%.

Le deuxième qubit (centré à 1532,2 nm) est envoyé à Bob qui le mesure avec son ATU tout-fibre (cf. section 4.4.2). Tout comme l'ATU d'Alice, supposons pour l'instant que la phase relative ϕ_B entre les bras de l'interféromètre est nulle. Ainsi, chaque détection survient dans la fenêtre temporelle f_2 avec une probabilité de 50%, ce qui correspond à mesurer dans la base

$$\{\cos\theta_B|t_0\rangle + \sin\theta_B|t_1\rangle, \sin\theta_B|t_0\rangle - \cos\theta_B|t_1\rangle\}. \tag{5.28}$$

Autrement, chaque détection survient dans la fenêtre f_0 avec une probabilité de 25%, ce qui correspond à une projection sur l'état $|t_0\rangle$, ou dans la fenêtre f_1 avec une probabilité de 25%, ce qui correspond à une projection sur $|t_1\rangle$.

5.11.2 Avantage de l'intrication

Une source à un photon peut, en principe, être réalisée de façon approximative en atténuant une impulsion laser cohérente jusqu'à ce que chaque impulsion contienne un nombre moyen de photon inférieur à 1. Or, nous avons montré à la section 5.6.6 comment l'utilisation d'une telle source rend notre implémentation non sécuritaire. Une option de rechange est d'utiliser l'intrication. En effet, une source de qubits photoniques intriqués basée sur une source de paires de photons obéissant à une distribution de Poisson est telle que l'état de chaque paire de photons est en pratique indépendant de toutes les autres. Ceci est bien entendu une approximation car même pour une source Poissonnienne, il existe une probabilité non-nulle, mais généralement très faible, que deux ou plusieurs paires soient créées à l'intérieur de leur temps de cohérence. Lorsque c'est le cas, l'émission stimulée est telle que les paires sont intriquées et donc que Bob pourrait potentiellement augmenter son biais en ne considérant que les cas où Alice prépare (involontairement) plus d'un qubit à l'intérieur du temps de cohérence (ceci nécessiterait un détecteur ayant un temps de réponse de l'ordre de 10^{-15} s pour résoudre le temps de cohérence). Cette situation est équivalente à celle où la source d'Alice suit une distribution thermique et nous en discutons plus loin.

Supposons pour l'instant que l'état de chaque paire soit séparable des autres. L'état global de N paires est

$$\left[\tfrac{1}{\sqrt{2}}(|t_0,t_0\rangle + |t_1,t_1\rangle)\right]^{\otimes N}. \tag{5.29}$$

Si les détecteurs d'Alice sont incapables de résoudre le nombre de photons et que la transmittance du canal entre le cristal et les détecteurs, incluant le rendement des détecteurs, est de 100%, alors Alice doit bien traiter les cas où elle enregistre un coup double à S_+ et à S_- (cf. fig. 4.9). En effet, supposons qu'Alice ignore les éxécutions où elle enregistre un coup

double. Cela implique qu'à chaque fois que deux qubits sont détectés dans le même détecteur et dans la même fenêtre temporelle, alors ils se retrouvent dans le même état. Comme Alice ignore que deux qubits ont été détectés, elle supposera qu'un seul qubit a été produit et continuera le protocole. Bob peut alors déterminer de façon concluante la base x et le bit a d'Alice et obtenir le résultat c de son choix avec certitude. La solution est de forcer Alice à continuer le protocole même si elle a enregistré une double détection et de choisir au hasard lequel des détecteurs elle va considérer pour déterminer l'état qu'elle a préparé. Ceci produira inévitablement des erreurs mais dont la quantité peut-être minimisée en diminuant le plus possible la probabilité d'émettre plusieurs paires.

En pratique, une transmittance totale de 100% n'existe pas. Qu'arrive-t-il dans ce cas si Alice ignore les doubles détections ? Supposons que le montage d'Alice soit bien équilibré et que chaque fois que la source émet une seule paire, la probabilité qu'elle détecte chacun des états du protocole soit égale à $\frac{1}{4}\eta$, où $0 < \eta < 1$. La quantité η correspond alors à la transmittance totale du canal d'Alice, soit la probabilité qu'un qubit émit par la source soit détecté par Alice. Lorsque la source émet deux paires indépendantes, la probabilité que les deux qubits d'Alice soient projetés sur le même état est

$$4 \times \left(\frac{1}{4}\eta\right)^2 = \frac{1}{4}\eta^2, \tag{5.30}$$

auquel cas les deux qubits envoyés chez Bob sont préparés dans le même état. D'autre part, la probabilité qu'un qubit donné soit détecté est η et la probabilité qu'il ne soit pas détecté est $(1-\eta)$. Pour deux qubits incidents chez Alice, la probabilité qu'un soit détecté et l'autre pas est donc $2\eta(1-\eta)$, auquel cas les états des qubits envoyés vers Bob sont complètement indépendants. Ainsi, à chaque fois que deux paires sont émises mais qu'un seul détecteur d'Alice réagit, la probabilité qu'il y ait eu double détection est

$$P = \frac{\frac{1}{4}\eta^2}{2\eta(1-\eta) + \frac{1}{4}\eta^2} = \frac{\eta}{8-7\eta}. \tag{5.31}$$

Pour $\eta < 3\%$, ce qui correspond à notre expérience (cf. section 3.5), $P < 0{,}4\%$. Dans le cas d'une double détection, les deux qubits envoyés à Bob sont dans le même état avec certitude. Par contre, si un seul des photons a été détecté par Alice, alors les deux qubits envoyés à Bob ne sont pas corrélés. La proportion totale des doubles qubits envoyés à Bob qui sont préparés dans le même état est donc

$$P \times 1 + (1-P) \times \frac{1}{4} < 25{,}3\%. \tag{5.32}$$

Ceci diffère très peu du cas où les états des deux qubits sont toujours indépendants et pour lequel la probabilité qu'ils soient préparés dans le même état est 25%.

Le fait que $\eta < 1$ empêche Bob de déterminer de façon concluante l'état des deux qubits car il n'a plus la certitude qu'ils sont préparés dans le même état. De plus, l'information qu'il peut extraire du fait que les qubits sont préparés dans le même état avec une probabilité d'au plus 25,3% au lieu de 25% est très faible et ne peut pas l'aider à augmenter son biais de façon significative. Nous supposons donc que l'information que Bob peut exploiter en tirant profit des impulsions à plusieurs photons est négligeable.

Supposons maintenant que la source d'Alice soit décrite par une distribution thermique. Tout comme le cas d'une source décrite par une distribution de Poisson, on doit forcer Alice à continuer le protocole même si elle a enregistré une double détection ; elle choisit au hasard lequel des détecteurs elle va considérer pour déterminer l'état qu'elle a préparé. Ainsi, Bob ne peut exploiter les impulsions contenant plus d'un qubit pour augmenter son biais. Si, par contre, Alice ignore les doubles détections, il est possible de montrer que, malgré cela, le biais de Bob ne peut être augmenté au-delà du biais correspondant à l'émission d'une seule paire. Ce calcul est fastidieux et sera présenté ailleurs.

Alice pourrait tenter de tricher lorsque les détecteurs de Bob sont incapables de résoudre le nombre de photons et qu'il ignore les doubles détections. Pour illustrer ceci, supposons que le choix de la base de mesure de Bob est un choix actif de sorte que tous les qubits reçus sont mesurés dans la même base. Si Alice envoie une impulsion contenant un très grand nombre de qubits tous préparés dans le même état et que les bases de préparation et de mesure ne sont pas les mêmes, alors Bob est presque assuré d'enregistrer une double détection et de déclarer une *erreur*. Par contre, si les bases de préparations et de mesure sont identiques, alors est il est fort probable qu'un seul des détecteurs de Bob n'enregistre un coup, auquel cas l'exécution ne sera pas avortée. Dans ce cas, Alice est presque certaine de la base dans laquelle Bob a mesuré et, pour obtenir le résultat désiré, elle n'a qu'à déclarer que son qubit a été envoyé dans l'autre base et Bob sera forcé d'accepter de continuer.

Dans notre expérience, le choix de la base de mesure de chaque qubit est réalisé passivement à l'aide de l'ATU de Bob. Ainsi, l'attaque décrite au paragraphe précédent ne s'applique pas. On peut cependant envisager qu'Alice envoie autre chose que plusieurs qubits préparés dans le même état et tenter d'augmenter son biais en tirant profit du fait que Bob ignore les doubles détections. Or, comme le rendement des détecteurs de Bob est de l'ordre de 25% ou moins, elle ne peut pas savoir avec certitude si tous les photons qu'elle a envoyés chez Bob ont été détectés ou pas et cela limite sévèrement l'efficacité de toute attaque de ce type. Au final, l'attaque basée sur la triche optimale semble être nettement plus efficace et le biais d'Alice ne peut pas être augmenté significativement au-delà du biais de cette attaque par

l'envoi d'impulsions à plusieurs photons chez Bob.

Les arguments donnés ici ne couvrent pas tous les cas possibles. Ceci est un problème complexe et il sera considéré ailleurs. Néanmoins, nous espérons que cette discussion convaincra le lecteur qu'une attaque exploitant les impulsions à plusieurs qubits émis d'une source d'intrication ne permet pas de briser le protocole de façon triviale.

5.11.3 Implémentation du pile ou face séquentiel

Nous avons utilisé notre source d'intrication pour implémenter un grand nombre d'exécutions de notre protocole de pile ou face quantique tolérant aux pertes, ce qui nous a permis de mesurer les performance de notre protocole et de réaliser la tâche du pile ou face séquentiel. Nous avons d'abord utilisé les états BB84 (cf. section 5.6.4) pour implémenter le protocole dans le cas où (1) Alice et Bob sont honnêtes, (2) Alice triche et Bob est honnête et (3) Bob triche et Alice est honnête. Ces trois cas ont ensuite été répétés avec les états équilibrés produisant en théorie un biais identique pour Alice et Bob (cf. section 5.6.5).

Comme pour les expériences relatées au chapitre 4, celles-ci ont d'abord été réalisées avec le montage de Bob placé directement aux côtés du montage d'Alice à l'Université de Calgary (UdeC) et où les photons étaient transmis sur une fibre à maintient de polarisation longue de 10 m, tel que décrit dans la section 4.4 (voir aussi la section 4.4.7). Puis, toutes les mesures ont été répétées après avoir déplacé le montage de Bob à SAIT où les photons étaient transmis sur la fibre optique souterraine de 12,4 km reliant l'UdeC et SAIT. Les imperfections et sources de bruit de notre source sont les mêmes que celles discutées au chapitre 4 (cf. sections 4.4 et 4.5).

On note que notre expérience est une implémentation complète de notre protocole et non pas une démonstration de principe.

Alice et Bob sont honnêtes

Lorsqu'Alice est honnête, son ATU est ajusté pour préparer un des états $|\alpha_{x,a}\rangle$ suivants, chacun avec une probabilité de 25% :

$$\left.\begin{array}{l} |\alpha_{0,0}\rangle = |t_0\rangle \\ |\alpha_{1,0}\rangle = |\alpha^+\rangle \end{array}\right\} \; a = 0$$
$$\left.\begin{array}{l} |\alpha_{0,1}\rangle = |t_1\rangle \\ |\alpha_{1,1}\rangle = |\alpha^-\rangle \end{array}\right\} \; a = 1\,, \tag{5.33}$$

où $|\alpha^+\rangle = \cos\alpha\,|t_0\rangle + \sin\alpha\,|t_1\rangle$, $|\alpha^-\rangle = \sin\alpha\,|t_0\rangle - \cos\alpha\,|t_1\rangle$ et $0° < \alpha \leq 45°$. Comme d'habitude, nous avons défini les bases

$$\tilde{\mathcal{B}}_x = \{|\alpha_{x,0}\rangle, |\alpha_{x,1}\rangle\}, \tag{5.34}$$

où $x \in \{0,1\}$ est utilisé pour identifier la base d'Alice. Lorsque $\alpha = 45°$, on obtient des états équivalents aux états BB84 et les bases $\tilde{\mathcal{B}}_0$ et $\tilde{\mathcal{B}}_1$ sont mutuellement non biaisées. Lorsque $\alpha = \arccos(4/5) \approx 36{,}9°$, on obtient des états équivalents aux états équilibrés et les bases $\tilde{\mathcal{B}}_0$ et $\tilde{\mathcal{B}}_1$ ne sont plus mutuellement non biaisées. Les états $|\alpha_{x,a}\rangle$ correspondants à ces deux cas sont montrés sur la fig. 5.3.

Lorsque Bob est honnête, son ATU est ajusté pour mesurer dans la base $\tilde{\mathcal{B}}_0$ avec une probabilité de 50% et dans la base $\tilde{\mathcal{B}}_1$ avec la probabilité complémentaire. Le choix de la base de mesure est fait de façon passive par l'ATU de Bob. Nous utiliserons $\hat{x} \in \{0,1\}$ pour

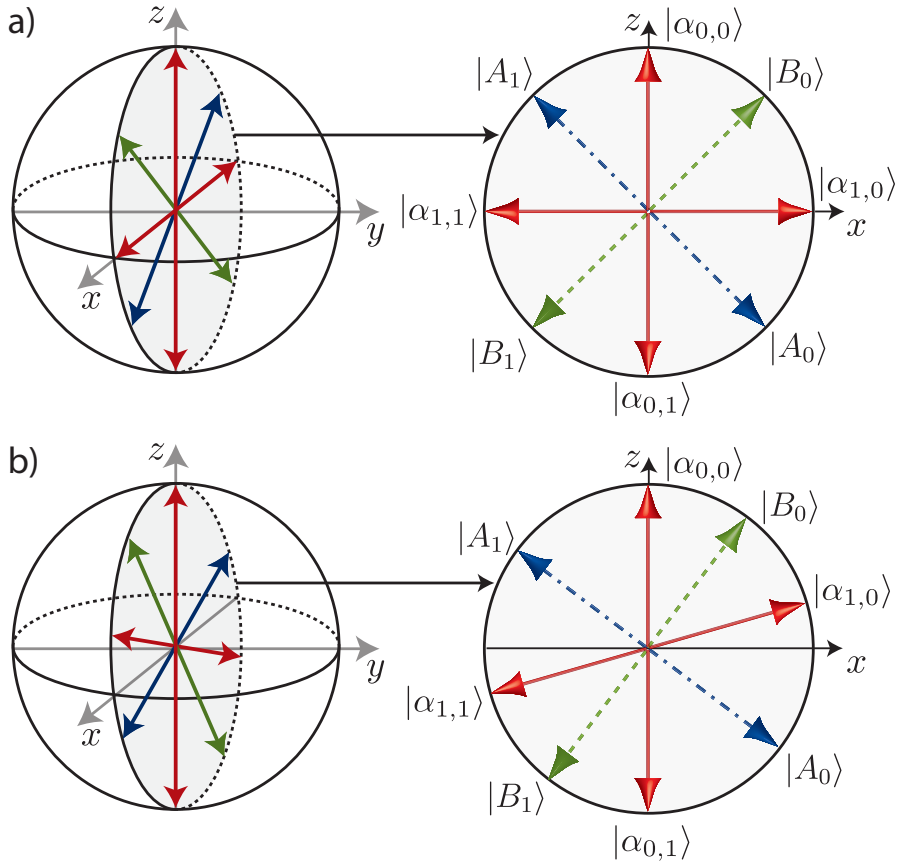

FIGURE 5.3 États $|\alpha_{x,a}\rangle$, $|A_0\rangle$, $|A_1\rangle$, $|B_0\rangle$ et $|B_1\rangle$ représentés sur la sphère de Bloch et sur le grand cercle x-z pour a) $\alpha = 45°$ et b) $\alpha \approx 36{,}9°$.

identifier la base dans laquelle Bob à mesuré.

Les étapes de l'implémentation de chaque éxécution du protocole honnête sont :

1. **Préparation de l'état par Alice :** le cristal NLPP est pompé par la diode laser (cf. Fig 4.9, page 83). Lorsque qu'un coup est enregistré au détecteur S_+ ou S_-, un signal « *det* » est émis par Alice et ce signal active les détecteurs I_+ et I_- de Bob. Le signal « *prêt* » démarre ensuite l'acquisition du convertisseur analogique-numérique temporel TDC-GPX. Le convertisseur enregistre le signal $S_+ \vee S_-$, ce qui permet de déterminer la fenêtre temporelle où le coup est survenu, et le signal $S_- \wedge hor$, ce qui permet de déterminer lequel des détecteurs d'Alice a enregistré le coup. Si le coup n'est pas survenu à l'intérieur d'une des trois fenêtres temporelles f_0, f_1 ou f_2 d'Alice, cette éxécution est ignorée. Autrement, le protocole continue. Ces informations, analysées en temps réel par une routine C++, permettent de déterminer lequel des états $|\alpha_{x,a}\rangle$ a été préparé par Alice.
2. **Mesure de Bob :** lorsque les détecteurs de Bob sont activés, les signaux I_+ et I_- sont enregistrés par le TDC-GPX. Si aucun coup n'est enregistré dans une des fenêtres f_0, f_1 ou f_2 de Bob, cette éxécution est ignorée. Sinon, les signaux I_+ et I_- sont utilisés par la routine pour déterminer lequel des détecteurs a enregistré le coup et dans quelle fenêtre temporelle cela est survenu. Ceci permet de déterminer la base $\hat{x}$ et le résultat $\hat{a} \in \{0, 1\}$ de la mesure de Bob.
3. **Bit aléatoire de Bob :** un bit pseudo-aléatoire b est généré par la routine.
4. **Résultat :** la routine compare d'abord x et $\hat{x}$. Si $x = \hat{x}$ et $a = \hat{a}$, le résultat du protocole est $c = a \oplus b$. Si $x = \hat{x}$ et $a \neq \hat{a}$, le résultat est une *erreur*. Si $x \neq \hat{x}$, le résultat est $c = a \oplus b$.

Pour implémenter le pile ou face séquentiel, un programme écrit avec le logiciel LabVIEW [12] est utilisé pour appeler séquentiellement la routine qui, à chaque exécution, retourne le résultat (c ou *erreur*), l'état déclaré par Alice $|\alpha_{x,a}\rangle$, la base $\hat{x}$ et le résultat $\hat{a}$ de la mesure de Bob. Ce programme compile les résultats et estime en temps réel la probabilité P_0 qu'une éxécution produise le résultat $c = 0$, la probabilité P_1 qu'elle produise $c = 1$ et la probabilité P^* qu'elle produise le résultat *erreur*. L'incertitude statistique sur chacune de ces quantités est calculée en supposant que chaque éxécution est indépendante de toutes les autres. Le programme estime aussi la probabilité qu'Alice prépare l'état $|\alpha_{x,a}\rangle$. Idéalement, celle-ci devrait être de 25% par état, mais en pratique des déviations de l'ordre de quelques points de pourcentage étaient parfois observées. Le programme estime finalement la probabilité que

12. Le logiciel LabVIEW fournit un environnement de programmation spécialisé dans la création d'interfaces entre un ordinateur et appareils de mesure et dans le traitement des données.

Bob mesure dans une base ou dans l'autre. Idéalement, on devrait obtenir 50% par base mais ici encore, une déviation de quelques points de pourcentage était parfois observée.

Alice triche et Bob est honnête

Lorsqu'Alice triche, son ATU est ajusté tel qu'une détection dans la fenêtre temporelle f_2 prépare un des états suivants avec la même probabilité pour chacun :

$$\begin{aligned} |A_0\rangle &= \cos\theta_A|t_0\rangle + \sin\theta_A|t_1\rangle \\ |A_1\rangle &= \sin\theta_A|t_0\rangle - \cos\theta_A|t_1\rangle\,. \end{aligned} \tag{5.35}$$

Alors qu'Alice et Bob devraient tous les deux utiliser les états BB84, Alice triche de façon optimale en choisissant $\theta_A = 67{,}5°$. Lorsqu'ils devraient utiliser les états équilibrés, Alice choisit plutôt $\theta_A = (90 + \arccos(4/5))/2 \approx 63{,}4°$. Les états $|A_0\rangle$ et $|A_1\rangle$ obtenus sont illustrés sur la fig. 5.3.

Les étapes de chaque éxécution du protocole où Alice triche sont :

1. **Préparation de l'état par Alice :** lorsqu'un coup est enregistré chez Alice, les détecteurs de Bob sont activés et l'acquisition des données par le TDC-GPX est démarrée. La routine C++ détermine la fenêtre temporelle de détection ainsi que lequel des détecteurs d'Alice a enregistré le coup. Si l'état préparé n'est pas $|A_0\rangle$ ou $|A_1\rangle$, cette éxécution est ignorée.
2. **Mesure de Bob :** si Bob enregistre un coup dans une des trois fenêtres temporelles f_0, f_1 ou f_2, la routine détermine la base $\hat{x}$ et le résultat $\hat{a}$ de Bob. Sinon, cette éxécution est ignorée.
3. **Bit aléatoire de Bob :** un bit pseudo-aléatoire b est généré par la routine.
4. **Déclaration d'Alice :** un bit pseudo-aléatoire c' est généré par la routine. Ce bit correspond au résultat désiré par Alice. Si $|A_i\rangle$ est l'état préparé par Alice, elle déclare $a = b \oplus c'$ et $x = a \oplus i \oplus 1$.
5. **Résultat :** la routine compare d'abord x et $\hat{x}$. Si $x = \hat{x}$ et $a = \hat{a}$, le résultat du protocole est $c = a \oplus b = c'$. Si $x = \hat{x}$ et $a \neq \hat{a}$, le résultat est *erreur*. Si $x \neq \hat{x}$, le résultat est $c = a \oplus b = c'$.

Le programme LabVIEW appelle séquentiellement la routine qui, pour chaque éxécution, retourne le résultat (c ou *erreur*), l'état $|\alpha_{x,a}\rangle$ déclaré par Alice, la base $\hat{x}$ et le résultat $\hat{a}$ de la mesure de Bob ainsi que l'état réellement préparé par Alice. Le programme compile les résultats et estime la probabilité P_A qu'Alice obtienne le résultat de son choix ainsi que la probabilité $P_A^* = 1 - P_A$ que Bob déclare une erreur. Cette probabilité devrait être égale

à $P_A^* = P^* + (1 - P^*)\left(\frac{1}{2} - \varepsilon_A\right)$, où ε_A est le bias d'Alice correspondant au protocole utilisé (éq. 5.23). Le programme estime aussi la probabilité qu'Alice prépare l'état $|A_0\rangle$ ou $|A_1\rangle$ par éxécution. Ces probabilités devraient idéalement être de 50% chacune, mais en pratique une variation de quelques points de pourcentage était parfois observée.

Bob triche et Alice est honnête

Lorsque Bob triche, son ATU est ajusté tel qu'une détection dans la fenêtre temporelle f_2 correspond à mesurer un des états suivants :

$$\begin{aligned} |B_0\rangle &= \cos\theta_B|t_0\rangle + \sin\theta_B|t_1\rangle \\ |B_1\rangle &= \sin\theta_B|t_0\rangle - \cos\theta_B|t_1\rangle\,. \end{aligned} \tag{5.36}$$

Alors qu'Alice et Bob devraient tous les deux utiliser les états BB84, Bob triche de façon optimale en choisissant $\theta_B = 22{,}5°$. Lorsqu'ils devraient utiliser les états équilibrés, Bob choisit plutôt $\theta_B = \arccos(4/5)/2 \approx 18{,}4°$. Les états $|B_0\rangle$ et $|B_1\rangle$ obtenus sont illustrés sur la fig. 5.3.

Les étapes de chaque éxécution du protocole où Bob triche sont :

1. **Préparation de l'état par Alice :** lorsqu'un coup est enregistré chez Alice, les détecteurs de Bob sont activés et l'acquisition des données par le TDC-GPX est démarrée. La routine C++ détermine l'état $|\alpha_{x,a}\rangle$ préparé par Alice.
2. **Mesure de Bob :** si Bob enregistre un coup dans la fenêtre temporelle f_2, la routine détermine l'état mesuré par Bob ($|B_0\rangle$ ou $|B_1\rangle$). Sinon, cette éxécution est ignorée.
3. **Bit de Bob :** un bit pseudo-aléatoire c' est généré par la routine. Ce bit correspond au résultat désiré par Bob. Si Bob a obtenu l'état $|B_i\rangle$, il déclare $b = i \oplus c'$.
4. **Résultat :** si $i = a$, le résultat est $c = a \oplus b = c'$. Si $i \neq a$, le résultat du protocole est *erreur*.

Le programme LabVIEW appelle séquentiellement la routine qui, pour chaque éxécution, retourne le résultat ($c = c'$ ou *erreur*), l'état $|\alpha_{x,a}\rangle$ préparé par Alice et l'état $|B_i\rangle$ mesuré par Bob. Le programme compile les résultats et détermine la probabilité P_B que Bob obtienne le résultat de son choix ainsi que la probabilité $P_B^* = 1 - P_B$ que Bob déclare une erreur. Cette probabilité devrait être égale à $P_B^* = P^* + (1 - P^*)\left(\frac{1}{2} - \varepsilon_B\right)$, où ε_B est le bias de Bob correspondant au protocole utilisé. Le programme estime aussi la probabilité que Bob mesure l'état $|B_0\rangle$ ou l'état $|B_1\rangle$ par éxécution. Ces probabilités devraient idéalement être de 50% chacune, mais en pratique une variation de quelques points de pourcentage était parfois observée.

Ajustement de la phase de l'interféromètre de Bob et stabilité

À la section 5.11.1 nous avons supposé que les phases ϕ_A et ϕ_B des interféromètres d'Alice et de Bob sont nulles. En général, cela est faux lorsque les interféromètres ne sont pas stabilisés de façon active. La conséquence directe est une préparation imparfaite du qubit de Bob et donc d'une augmentation du taux d'erreur du protocole. Pour voir ceci, on remarque que cette situation est équivalente à celle où l'état des qubits intriqués créés par la source d'Alice est

$$\frac{1}{\sqrt{2}}(|t_0, t_0\rangle + \mathrm{e}^{-i(\phi_A+\phi_B)}|t_1, t_1\rangle) \tag{5.37}$$

au lieu de $\frac{1}{\sqrt{2}}(|t_0, t_0\rangle + |t_1, t_1\rangle)$. Lorsque l'ATU d'Alice projette son qubit sur l'état $|\alpha^+\rangle = \cos\alpha|t_0\rangle + \sin\alpha|t_1\rangle$, le qubit de Bob est préparé dans l'état $\cos\alpha|t_0\rangle + \mathrm{e}^{-i(\phi_A+\phi_B)}\sin\alpha|t_1\rangle \neq |\alpha^+\rangle$, ce qui ne peut qu'augmenter le taux d'erreur du protocole. Cette augmentation peut être minimisée en faisant varier la tension appliquée sur l'actuateur piézoélectrique PZ de l'ATU tout-fibre de Bob (cf. fig. 4.8) jusqu'à l'obtention du taux d'erreur P^* minimal ; ceci implique que $\phi_B \approx -\phi_A$ et que la phase relative est annulée.

Cet ajustement de la phase relative était réalisé avant chaque réalisation du pile ou face séquentiel. Le temps maximal de mesure suivant chaque ajustement était de 10 minutes, ce qui assurait une stabilité interférométrique suffisante.

Avantage des ATU

Tous les états utilisés pour implémenter notre protocole sont contenus sur le même grand cercle de la sphère de Bloch. L'utilisation des ATU n'était donc pas nécessaire car en principe nous aurions pu utiliser des analyseurs temporels contraints à projeter sur des états de l'équateur de la sphère de Bloch (cf. fig. 2.2). Cela aurait cependant nécessité soit l'utilisation de 8 détecteurs au lieu de 4, soit l'utilisation d'un choix de base actif à l'aide d'un modulateur de phase installé dans l'un des bras de l'analyseur temporel contraint. Ces deux options sont technologiquement plus complexes et coûteuses que celle basée sur l'utilisation des ATU.

5.12 Résultats expérimentaux

Dans cette section, nous présentons les résultats du pile ou face séquentiel. Les cas où Alice et Bob sont honnêtes, Alice triche et Bob triche sont d'abord discutés séparément. Tous les résultats importants sont ensuite comparés entre eux.

Alice et Bob sont honnêtes

Nous avons estimé les probabilités P_0, P_1 et P^* avec les états BB84 et les états équilibrés lorsque Bob était d'abord à l'UdeC et ensuite à SAIT. Les résultats complets sont présentés au tableau 5.1 et la fig. 5.4 permet de comparer visuellement la différence entre les résultats obtenus lorsque Bob était à l'UdeC et lorsqu'il se trouvait à SAIT.

On remarque premièrement que $P^* < 2\%$ avec Bob à l'UdeC et $P^* < 5\%$ avec Bob à SAIT. L'augmentation du taux d'erreur en passant du premier cas au deuxième est causée par la diminution du rapport signal sur bruit et donc à l'augmentation de la contribution des coups sombres (cf. section 4.5.2). Il est aussi intéressant de comparer P^* avec le taux maximal $P^*_{\max}$ au-delà duquel il est possible que le tricheur ait choisi le résultat de tous les bits de la séquence,

TABLEAU 5.1 Résultats du pile ou face séquentiel lorsqu'Alice et Bob sont honnêtes. La colonne de gauche indique les états utilisés (BB84 ou équilibrés) ainsi que l'endroit où se trouvait Bob (UdeC ou SAIT). La dernière colonne N_{ex} indique le nombre d'exécutions de la séquence. L'incertitude sur chaque quantité est statistique.

	$P_0 \pm \Delta P_0$ (%)	$P_1 \pm \Delta P_1$ (%)	$P^* \pm \Delta P^*$ (%)	$P^*_{\max}$ (%)	N_{ex} ($\times 10^3$)
BB84 - UdeC	$49{,}1 \pm 0{,}1$	$49{,}2 \pm 0{,}1$	$1{,}72 \pm 0{,}04$	7,3 ou 14,6	118,4
BB84 - SAIT	$47{,}3 \pm 0{,}3$	$48{,}1 \pm 0{,}3$	$4{,}5 \pm 0{,}1$	7,3 ou 14,6	30,4
Équi. - UdeC	$48{,}9 \pm 0{,}1$	$49{,}2 \pm 0{,}1$	$1{,}92 \pm 0{,}04$	10	116,1
Équi. - SAIT	$47{,}4 \pm 0{,}3$	$47{,}9 \pm 0{,}3$	$4{,}6 \pm 0{,}1$	10	22,5

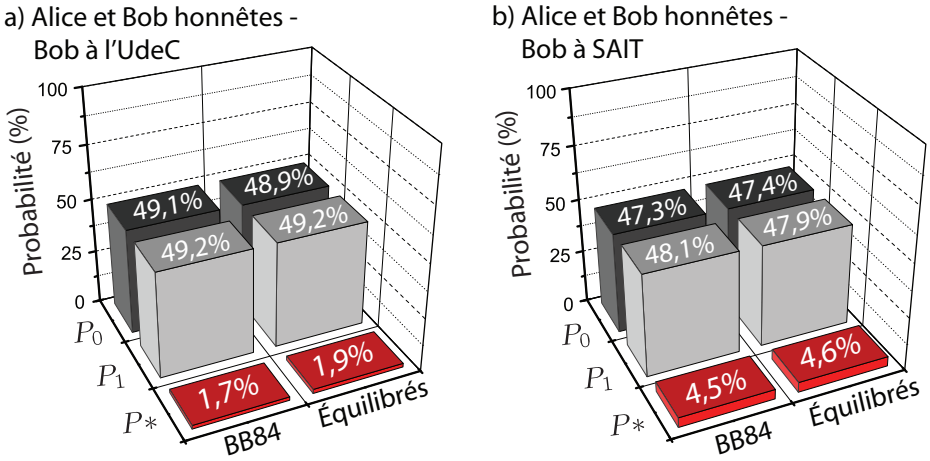

FIGURE 5.4 Histogrammes compilant les résultats du pile ou face séquentiel lorsqu'Alice et Bob sont honnêtes lorsque Bob est a) à l'UdeC et b) à SAIT.

tel qu'expliqué à la section 5.9. Pour les états BB84 on a $P^*_{\max} \approx (100 - 92{,}7)\% = 7{,}3\%$ lorsqu'Alice triche et $P^*_{\max} \approx (100 - 85{,}4)\% = 14{,}6\%$ lorsque Bob triche. Pour les états équilibrés, on a $P^*_{\max} = (100 - 90)\% = 10\%$. Dans tous les cas, nous avons mesuré que $P^* < P^*_{\max}$. Par conséquent, la sécurité du pile ou face séquentiel n'est donc pas compromise malgré les pertes et le bruit. On remarque deuxièmement que les probabilités P_0 et P_1 sont égales à un ou deux écart-types près et donc que le protocole génère bien un bit aléatoire.

Alice triche et Bob est honnête

Nous avons mesuré la probabilité P_A qu'Alice réussisse à obtenir le résultat désiré par exécution ainsi que la probabilité P^*_A que Bob déclare une erreur. Les valeurs obtenues sont présentées au tableau 5.2. (La fig. 5.5 présente ces valeurs sous forme d'histogrammes et est discutée ci-dessous.) Premièrement, il est intéressant de comparer chaque valeur de P_A avec la valeur maximale théorique « P_A (th.) » correspondante. Tel que prévu, P_A est inférieure au maximum théorique en raison du bruit intrinsèque du montage expérimental. Par conséquent, les valeurs de P^*_A, correspondant à la probabilité que Bob déclare une erreur, sont toutes plus élevées que les valeurs minimales théoriquement possibles de la colonne « P^*_A (th.) ». On remarque ensuite que les valeurs de P^*_A sont toutes significativement plus élevées que le taux d'erreur intrinsèque du montage P^*. Ceci démontre que notre protocole est sécuritaire contre une Alice tricheuse et que Bob se rendrait compte qu'Alice a choisi chacun des bits de la séquence générée en estimant cette probabilité. Deuxièmement, on remarque que la valeur de P_A obtenue dans le cas « BB84 - UdeC », $(91{,}1 \pm 0{,}1)\%$, est nettement supérieure à 90%. Nous avons donc démontré qu'Alice peut tricher de façon plus efficace avec les états BB84 que ce qui est théoriquement possible avec les états équilibrés. Finalement, la colonne « P^*_A (cont) » nous donne la contribution de la triche d'Alice au taux d'erreur total mesuré. Pour

Tableau 5.2 Résultats du pile ou face séquentiel lorsqu'Alice triche et Bob est honnête. L'incertitude sur chaque quantité est statistique sauf celle de « P^*_A (cont) » qui provient d'un calcul de propagation des incertitudes.

	$P_A \pm \Delta P_A$ (%)	P_A (th.) (%)	$P^*_A \pm \Delta P^*_A$ (%)	P^*_A (th.) (%)	P^*_A (cont) (%)	N_{ex} ($\times 10^3$)
BB84 - UdeC	$91{,}1 \pm 0{,}1$	92,7	$8{,}9 \pm 0{,}1$	7,3	$7{,}3 \pm 0{,}1$	82,7
BB84 - SAIT	$89{,}5 \pm 0{,}3$	92,7	$10{,}5 \pm 0{,}3$	7,3	$6{,}2 \pm 0{,}3$	9,5
Équi. - UdeC	$88{,}2 \pm 0{,}1$	90	$11{,}8 \pm 0{,}1$	10	$10{,}0 \pm 0{,}1$	77,4
Équi. - SAIT	$85{,}4 \pm 0{,}3$	90	$14{,}6 \pm 0{,}3$	10	$10{,}5 \pm 0{,}3$	18,7

calculer ceci, on définit

$$P_A^*\,(\text{cont}) = \frac{(P_A^* - P^*)}{1 - P^*}. \tag{5.38}$$

En comparant cette définition avec l'éq. 5.23, on voit que « P_A^* (cont) » devrait être égale à « P_A^* (th.) ». C'est bien ce qu'on obtient lorsque Bob était à l'UdeC. Les valeurs obtenues lorsque Bob était à SAIT sont légèrement décalées de la prédiction théorique. Il est possible que, pour ces mesures, la phase ϕ_B de l'ATU de Bob n'a pas été ajustée de façon optimale, ce qui expliquerait le décalage observé (cf. section 5.11.3).

Bob triche et Alice est honnête

Nous avons mesuré la probabilité P_B que Bob réussisse à obtenir le résultat désiré par exécution ainsi que la probabilité P_B^* que Bob déclare une erreur. Les valeurs obtenues sont présentées au tableau 5.3. La fig. 5.5 présente ces valeurs sous forme d'histogrammes. Premièrement, on peut comparer chaque valeur de P_B avec la valeur maximale théorique « P_B (th.) » correspondante. Tel que prévu, P_B est inférieure au maximum théorique en raison du bruit intrinsèque du montage expérimental. Les valeurs de P_B^* sont toutes plus élevées que les valeurs minimales théoriquement possibles de la colonne « P_B^* (th.) » et toutes significativement plus élevées que le taux d'erreur intrinsèque du montage P^*. Ceci démontre que notre protocole est sécuritaire contre un Bob tricheur et qu'Alice se rendrait compte que Bob a choisi chacun des bits de la séquence générée en estimant cette probabilité. Deuxièmement, on remarque que la valeur de P_B obtenue dans le cas « Équi. - UdeC », $(88{,}4 \pm 0{,}1)\%$, est nettement supérieure à 85,4%. Nous avons donc démontré que Bob peut tricher de façon plus efficace avec les états équilibrés que ce qui est théoriquement possible avec les états BB84. Finalement, la quantité

$$P_B^*\,(\text{cont}) = \frac{(P_B^* - P^*)}{1 - P^*}, \tag{5.39}$$

Tableau 5.3 Résultats du pile ou face séquentiel lorsque Bob triche et Alice est honnête. L'incertitude sur chaque quantité est statistique sauf celle de « P_B^* (cont) » qui provient d'un calcul de propagation des incertitudes.

	$P_B \pm \Delta P_B$ (%)	P_B (th.) (%)	$P_B^* \pm \Delta P_B^*$ (%)	P_B^* (th.) (%)	P_B^* (cont) (%)	N_{ex} ($\times 10^3$)
BB84 - UdeC	$83{,}8 \pm 0{,}1$	85,4	$16{,}2 \pm 0{,}1$	14,6	$14{,}7 \pm 0{,}1$	79,5
BB84 - SAIT	$81{,}4 \pm 0{,}5$	85,4	$18{,}6 \pm 0{,}5$	14,6	$14{,}7 \pm 0{,}5$	7,1
Équi. - UdeC	$88{,}4 \pm 0{,}1$	90	$11{,}6 \pm 0{,}1$	10	$9{,}8 \pm 0{,}1$	77,9
Équi. - SAIT	$85{,}4 \pm 0{,}4$	90	$14{,}6 \pm 0{,}4$	10	$10{,}4 \pm 0{,}4$	7,9

nous donne la contribution de la triche de Bob au taux d'erreur total mesuré et devrait être égale à « P_B^* (th.) ». C'est bien ce qu'on obtient en tenant compte de l'incertitude statistique.

Effet du canal de transmission et des états en présence d'un tricheur

Les résultats obtenus en présence d'un tricheur sont résumés visuellement à la fig. 5.5. L'effet du canal de transmission sur les performances du protocole est apparente lorsqu'on compare respectivement les cas a) et c) avec b) et d) : les probabilités P_A^* et P_B^* augmentent en raison de la diminution du rapport signal sur bruit et, par conséquent, les probabilités P_A et P_B diminuent. L'effet du choix des états utilisés sur la sécurité est apparente lorsqu'on compare respectivement les cas a) et b) avec c) et d) : le passage des états BB84 vers les états équilibrés diminue la probabilité P_A tandis qu'elle augmente la probabilité P_B, ce qui a pour effet d'équilibrer les biais d'Alice et de Bob.

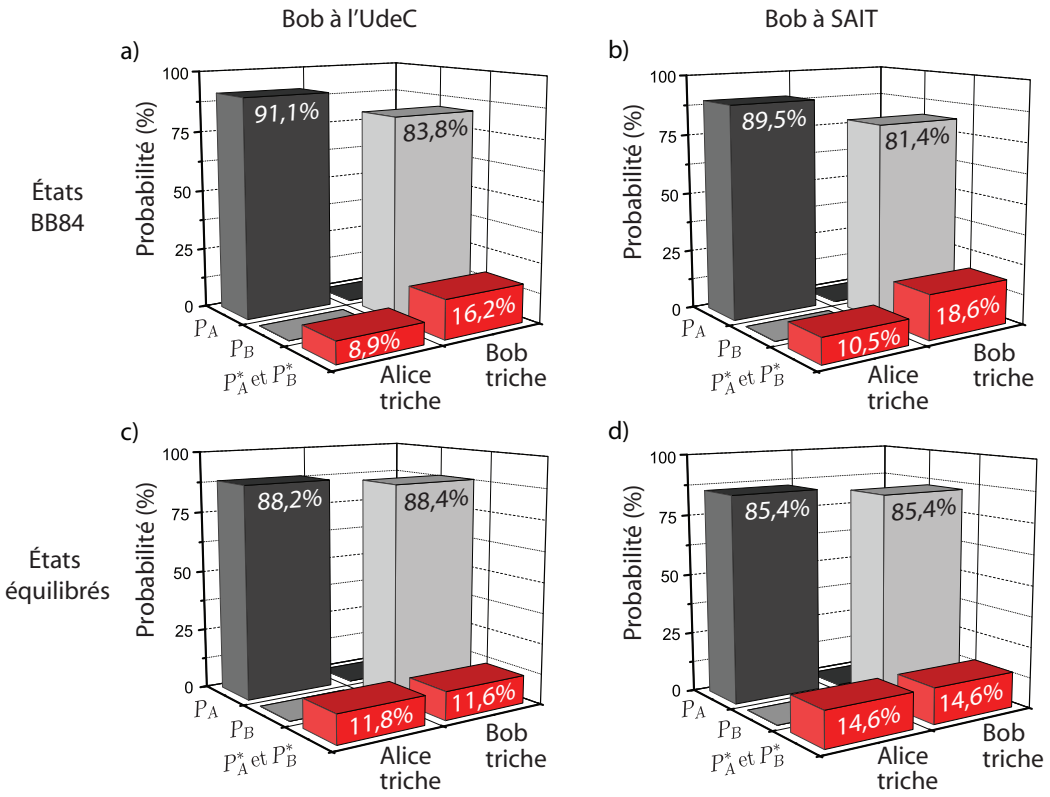

FIGURE 5.5 Histogrammes compilant les résultats du pile ou face séquentiel en présence d'un tricheur.

5.13 Résumé de la partie expérimentale

Les résultats expérimentaux présentés montrent clairement que la tâche du pile ou face séquentiel peut être réalisée avec la technologie actuelle dans un contexte réaliste où les photons sont transmis sur une fibre optique souterraine. Plusieurs questions restent en suspens, notamment celle de la sécurité de la tâche de pile ou face séquentiel basée sur l'échange asynchrone d'information classique seulement. Nous avons conjecturé à la section 5.9 que cela est impossible à réaliser de façon inconditionnellement sécuritaire et donné des arguments préliminaires mais une preuve formelle de cette impossibilité ou possibilité reste à faire. D'autre part, une étude exhaustive de la sécurité de l'implémentation où les qubits sont générés à partir d'une source d'intrication émettant parfois plus d'une paire doit être complétée. Ici encore, nous avons présenté à la section 5.11.2 quelques arguments suggérant que la sécurité n'est pas compromise mais cette étude reste préliminaire.

Chapitre 6

Conclusion

La communication quantique permet, dans certaines situations, de repousser les limites de la communication classique. Cette thèse a présenté des avancées théoriques et technologiques appliquées à la communication quantique dans un contexte réaliste avec essais *sur le terrain*. Les innovations présentées élargissent le champ d'application de l'intrication temporelle à travers l'élaboration (i) de nouvelles méthodes pour manipuler l'encodage temporel, (ii) d'un nouveau modèle de caractérisation d'une source de paires de photons, (iii) de nouvelles façons d'étudier la non-localité de l'intrication temporelle et (iv) du premier protocole de pile ou face quantique tolérant aux pertes et de sa réalisation expérimentale. Les contributions, les limitations et les nouvelles voies de recherche issues des travaux de chaque chapitre sont présentées ici.

Manipulation de l'encodage temporel

Nous avons proposé deux méthodes permettant d'implémenter une opération unitaire, arbitraire et déterministe sur un qubit temporel à l'aide de composants optiques tout-fibre. Nous avons montré comment réaliser un analyseur temporel universel (ATU) permettant de mesurer un qubit temporel dans une base arbitraire. Ces méthodes ont été généralisées au cas d'un qudit temporel. Nous avons appliqué ces propositions au cas spécifique du *calcul quantique basé sur la mesure* avec une une architecture tout-fibre et montré comment réaliser les *opérations en aval* essentielles à cette approche. Ces travaux ouvrent la voie vers la création d'un ordinateur quantique basé sur l'optique, mais également vers de nouvelles tâches en communication quantique. En particulier, la méthode de l'ATU a été utilisée en combinaison avec la source d'intrication temporelle que nous avons réalisée. La réalisation des opérations unitaires arbitraires pose un défi technologique important en raison des pertes des composantes optiques et des problèmes reliés à la stabilisation de la phase des interféromètres. Ces limitations pourraient être surmontées en réduisant considérablement le délai des interféromètres ce qui nécessiterait aussi l'utilisation appareils tels que des détecteurs à un photon ayant une résolution temporelle bien inférieure à 1 ns. Une autre possibilité serait d'utiliser une technologie monolithique permettant de concentrer en bloc les circuits optique. Ces différentes approches permettront certainement, dans un avenir rapproché, de démontrer quelques unes des idées présentées ici.

Caractérisation d'une source de paires de photons

Nous avons présenté un modèle décrivant les statistiques des coups d'une source probabiliste de paires de photons. À l'aide de ce modèle, une méthode simple et rapide permettant d'estimer la luminosité de la source ainsi que la transmittance des canaux de transmission a été dérivée. Cette méthode a été appliquée à une source basée sur la conversion paramétrique spontanée dans un cristal de niobate de lithium ($LiNbO_3$) « polé » périodiquement et produisant des paires de photons à 812 et 1532 nm. La validité et la précision de notre modèle a été démontrée en comparant la prédiction et la mesure directe de l'autocorrélation de second ordre $g^{(2)}(0)$ d'une source de photons annoncés. Cette méthode pourra être utilisée pour ajuster la luminosité sur demande et en temps réel dans le but d'optimiser les performances de la distribution quantique de clés (DQC) basée sur l'intrication, de déterminer la sécurité de la DQC basée sur une source de photons annoncés et d'optimiser les performances d'un répéteur quantique. La première limitation de cette méthode est qu'elle nécessite la connaissance de la distribution statistique du nombre de paires de photons émises pour que les estimations de la luminosité et des transmittances soient justes. La deuxième est que la luminosité peut, dans certains cas, être surestimée si les photons sont corrélés en fréquence.

Non-localité d'une source d'intrication temporelle

Nous avons caractérisé une source d'intrication temporelle à l'aide d'analyseurs temporels universels. La présence de l'intrication a été révélée par la mesure de la visibilité de l'intrication. Cette mesure a été répétée plusieurs fois en utilisant différentes bases qui, lorsque disposées sur la sphère de Bloch, couvrent toutes les dimensions de cette dernière, mettant ainsi en évidence le caractère universel des analyseurs temporels universels (ATU). Nous avons ensuite révélé la nature non-locale de notre source d'intrication temporelle avec un test de l'inégalité de Bell-CHSH. Grâce aux ATU, ce test a pu être répété plusieurs fois de sorte que, de test en test, le grand cercle de la sphère de Bloch contenant les bases de mesures utilisées pour un test donné était soumis à une rotation. L'ensemble des grands cercles utilisés couvre toutes les dimensions de la sphère de Bloch. Ceci nous a permis de vérifier directement que la valeur du paramètre S est invariante par rotation du grand cercle contenant les bases de mesure. Ces expériences ont d'abord été réalisées dans l'environnement contrôlé d'un laboratoire, puis répétées sur le terrain. Elles nous ont permis de vérifier que les corrélations non-locales quantiques ne sont pas affectées par la transmission d'un des qubits sur 12,4 km de fibre optique souterraine.

Cette source peut aussi être interprétée comme une source d'*intrication hybride* où un qubit de polarisation est intriqué avec un qubit temporel. Elle pourrait s'avérer utile dans un réseau quantique composé de différents types de liens de transmission nécessitant différents types d'encodage. Finalement, ces travaux ouvrent aussi la voie vers de nouveaux tests

de la non-localité avec intrication temporelle, tels une inégalité de Leggett et l'inégalité « élégante », et vers la réalisation de nouveaux protocoles de communication quantique utilisant l'intrication temporelle, tels que le protocole de pile ou face quantique que nous avons réalisé. La principale limitation d'une source d'intrication temporelle réside dans le fait que, sans stabilisation active des interféromètres, le temps de mesure est limité, ce qui augmente l'incertitude statistique et réduit l'écart statistique entre le paramètre S observé et la borne de l'inégalité de Bell-CHSH.

Pile ou face quantique

Nous avons présenté le premier protocole de pile ou face quantique *tolérant aux pertes*. Nous avons montré comment équilibrer ce protocole et présenté les stratégies de triche optimales. Nous avons ensuite discuté des conséquences du bruit dans un montage réaliste et nous avons présenté une nouvelle tâche, nommée *pile ou face séquentiel*, basée sur l'application répétée de notre protocole de pile ou face quantique. Cette tâche est telle que sa sécurité n'est pas compromise en présence de pertes et de bruit. Finalement, à l'aide de notre source d'intrication temporelle et des analyseurs temporels universels, nous avons réalisé la première démonstration expérimentale d'un protocole de pile ou face quantique tolérant aux pertes et l'avons utilisé pour réaliser la tâche de pile ou face séquentiel. Ces expériences ont d'abord été réalisées dans l'environnement contrôlé d'un laboratoire, puis répétées sur le terrain où un des photons de chaque paire est transmis sur une fibre optique souterraine de 12,4 km. Plusieurs questions émergent de ces travaux. Elles sont énumérées ici.

- Quel est le plus petit biais possible d'un protocole tolérant aux pertes ? Autrement dit, est-ce que le biais de 0,4 de notre protocole est optimal ou bien existe-t-il un protocole avec un biais inférieur ?
- Existe-t-il un protocole de pile ou face quantique tolérant aux pertes dont le biais est inférieur à la borne de Kitaev, ou encore avec un biais arbitrairement près de 0 ?
- Pouvons-nous prouver que notre protocole est sécuritaire contre n'importe quelle attaque où Alice ou Bob exploitent les imperfections du montage (autres que le bruit), par exemple fait que la source d'intrication génère parfois plus d'une paire et que les détecteurs utilisés sont incapables de résoudre le nombre de photon, etc.
- Pouvons nous prouver que le pile ou face séquentiel est impossible classiquement ?
- Existe-t-il un protocole de pile ou face quantique tolérant au bruit ?

Références

[1] « Information society ». http://en.wikipedia.org/wiki/Information_society.

[2] « Internet World Stats ». http://www.internetworldstats.com/.

[3] C. H. Bennett et G. Brassard, « Quantum cryptography : public key distribution and coin tossing », *Proceedings of the International conference on Computers, Systems & Signal Processing, Bangalore, India*, pp. 175–179, 1984.

[4] M. A. Nielsen et I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[5] IdQuantique. http://www.idquantique.com/.

[6] MagiQ. http://www.magiqtech.com/.

[7] SmartQuantum. http://www.smartquantum.com/.

[8] W. Tittel et G. Weihs, « Photonic Entanglement for Fundamental Tests and Quantum Communication », *Quantum Inf. and Comp.*, vol. 1, no. 2, pp. 3–56, 2001.

[9] N. Gisin, G. Ribordy, W. Tittel et H. Zbinden, « Quantum Cryptography », *Reviews of Modern Physics*, vol. 74, pp. 145–195, 2002.

[10] N. Gisin et R. Thew, « Quantum communication », *Nature Photonics*, vol. 1, pp. 165–171, 2007.

[11] N. D. Mermin, *Quantum Computer Science : An Introduction*. Cambridge University Press, 2007.

[12] C. E. Shannon, « A mathematical theory of communication », *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.

[13] C. Cohen-Tannoudji, B. Diu et F. Laloë, *Mécanique quantique*. Hermann, 1996.

[14] W. K. Wootters et W. H. Zurek, « A single quantum cannot be cloned », *Nature*, vol. 299, pp. 802–803, 1982.

[15] D. Dieks, « Communication by EPR devices », *Physics Letters A*, vol. 6, no. 22, pp. 271–272, 1982.

[16] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa et B. Schumacher., « Noncommuting mixed states cannot be broadcast », *Physical Review Letters*, vol. 76, no. 15, pp. 2818–2821, 1996.

[17] S. L. Braunstein et P. van Loock, « Quantum information with continuous variables », *Reviews of Modern Physics*, vol. 77, no. 2, pp. 513–577, 2005.

[18] J. Brendel, N. Gisin, W. Tittel et H. Zbinden, « Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication », *Physical Review Letters*, vol. 82, no. 12, pp. 2594–2597, 1999.

[19] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko et Y. Shih, « New high-intensity source of polarization-entangled photon pairs », *Physical Review Letters*, vol. 75, no. 24, pp. 4337–4341, 1995.

[20] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum et P. H. Eberhard, « Ultra-bright source of polarization-entangled photons », *Physical Review A*, vol. 60, no. 2, pp. R773–R776, 1999.

[21] A. Einstein, B. Podolsky et N. Rosen, « Can quantum-mechanical description of physical reality be considered complete ? », *Physical Review*, vol. 47, no. 10, p. 777, 1935.

[22] J. S. Bell, « On the Einstein-Podolsky-Rosen paradox », *Physics*, vol. 1, pp. 195–200, 1964.

[23] D. Bohm et Y. Aharonov, « Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky », *Physical Review*, vol. 108, no. 4, pp. 1070–1076, 1957.

[24] J. F. Clauser, M. A. Horne, A. Shimony et R. A. Holt, « Proposed Experiment to Test Local Hidden-Variable Theories », *Physical Review Letters*, vol. 23, no. 15, pp. 880–884, 1969.

[25] S. J. Freedman et J. F. Clauser, « Experimental test of local hidden-variable theories », *Physical Review Letters*, vol. 28, no. 14, pp. 938–941, 1972.

[26] A. Aspect, P. Grangier et G. Roger, « Experimental tests of realistic local theories via Bell's theorem », *Physical Review Letters*, vol. 47, no. 7, pp. 460–463, 1981.

[27] A. Aspect, P. Grangier et G. Roger, « Experimental realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment* : A new violation of Bell's inequalities », *Physical Review Letters*, vol. 49, no. 2, pp. 91–94, 1982.

[28] A. Aspect, J. Dalibard et G. Roger, « Experimental test of Bell's inequalities using time- varying analyzers », *Physical Review Letters*, vol. 49, no. 25, pp. 1804–1807, 1982.

[29] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter et A. Zeilinger, « Violation of Bell's inequality under strict Einstein locality conditions », *Physical Review Letters*, vol. 81, no. 23, pp. 5039–5043, 1998.

[30] J. Brendel, E. Mohler et W. Martienssen, « Experimental test of Bell's inequality for energy and time », *Europhysics Letters*, vol. 20, pp. 575–580, 1992.

[31] P. G. Kwiat, A. M. Steinberg, et R. Y. Chiao, « High-visibility interference in a Bell-inequality experiment for energy and time », *Physical Review A*, vol. 47, no. 4, pp. R2472–R2475, 1993.

[32] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden et N. Gisin, « Experimental demonstration of quantum correlations over more than 10 km », *Physical Review A*, vol. 57, no. 5, pp. 3229–3232, 1998.

[33] W. Tittel, J. Brendel, H. Zbinden et N. Gisin, « Violation of Bell inequalities by photons more than 10 km apart », *Physical Review Letters*, vol. 81, no. 17, pp. 3563–3566, 1998.

[34] A. J. Leggett, « Nonlocal hidden-variable theories and quantum mechanics : An incompatibility theorem », *Foundations of Physics*, vol. 33, no. 10, pp. 1469–1493, 2003.

[35] C. Branciard, N. Brunner, N. Gisin, C. Kurtsiefer, A. Lamas-Linares, A. Ling et V. Scarani, « Testing quantum correlations versus single-particle properties within Leggett's model and beyond », *Nature Physics*, vol. 4, pp. 681–685, 2008.

[36] D. Greenberger, M. A. Horne et A. Zeilinger, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*. Kluwer Academic, Dordrecht, The Netherlands, 1989.

[37] N. D. Mermin, « Extreme quantum entanglement in a superposition of macroscopically distinct states », *Physical Review Letters*, vol. 65, no. 15, pp. 1838–1840, 1990.

[38] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski et A. Zeilinger, « Violations of Local Realism by Two Entangled n-Dimensional Systems Are Stronger than for Two Qubits », *Physical Review Letters*, vol. 85, no. 21, pp. 4418–4421, 2000.

[39] G. Brassard, R. Cleve et A. Tapp, « Cost of exactly simulating quantum entanglement with classical communication », *Physical Review Letters*, vol. 83, no. 9, pp. 1874–1877, 1999.

[40] G. Brassard, A. Broadbent et A. Tapp, « Quantum pseudo-telepathy », *Foundations of Physics*, vol. 35, no. 11, pp. 1877–1907, 2005.

[41] « Cryptography ». `http://en.wikipedia.org/wiki/Cryptography`.

[42] D. Stinson, *Cryptography - Theory and Practice,*. CRC Press, 2000.

[43] R. L. Rivest, A. Shamir et L. Adleman., « A method for obtaining digital signatures and public key cryptosystems », *Communications of the ACM*, vol. 21, pp. 120–126, 1978.

[44] S. J. Wiesner, « Conjugate coding », *Sigact News*, vol. 15, pp. 78–88, 1993.

[45] J. L. Carter et M. N. Wegman, « Universal classes of hash functions », *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[46] J. L. Carter et M. N. Wegman, « New hash functions and their use in authentication and set equality », *Journal of Computer and System Sciences*, vol. 22, no. 3, pp. 265–279, 1981.

[47] C. H. Bennett, G. Brassard et J.-M. Robert, « Privacy amplification by public discussion », *SIAM Journal on Computing*, vol. 17, pp. 210–229, 1988.

[48] C. H. Bennett, G. Brassard, C. Crépeau et U. M. Maurer, « Generalized privacy amplification », *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[49] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus et M. Peev, « The security of practical quantum key distribution ». `arXiv:0802.4155`, 2008.

[50] M. Blum, « Coin flipping by telephone : A protocol for solving impossible problems », *Advances in Cryptology : A Report on CRYPTO'81, Santa Barbara, California, USA*, pp. 11–15, 1981.

[51] H.-K. Lo et H. F. Chau, « Why quantum bit commitment and ideal quantum coin tossing are impossible », *Physica D*, vol. 120, pp. 177–187, 1998.

[52] D. Mayers, L. Salvail et Y. Chiba-Kohno, « Unconditionally secure quantum coin tossing ». `arXiv:quant-ph/9904078`, 1999.

[53] A. Kitaev, « A negative result abour quantum coin flipping ». `http://www.msri.org/publications/video/index05.html`. Présentation donnée à QIP 2003, MSRI, Berkeley, CA.

[54] J. Barrett et S. Massar, « Quantum coin tossing and bit-string generation in the presence of noise », *Physical Review A*, vol. 69, no. 2, p. 022322, 2004.

[55] A. K. Ekert, « Quantum cryptography based on Bell's theorem », *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[56] C. H. Bennett, G. Brassard et N. D. Mermin, « Quantum cryptography without Bell's theorem », *Physical Review Letters*, vol. 68, no. 5, pp. 557–559, 1992.

[57] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter et A. Zeilinger, « Quantum cryptography with entangled photons », *Physical Review Letters*, vol. 84, no. 20, pp. 4729–4732, 2000.

[58] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund et P. G. Kwiat, « Entangled state quantum cryptography : Eavesdropping on the Ekert protocol », *Physical Review Letters*, vol. 84, no. 20, pp. 4733–4736, 2000.

[59] W. Tittel, J. Brendel, H. Zbinden et N. Gisin, « Quantum cryptography using entangled photons in energy-time Bell states », *Physical Review Letters*, vol. 84, no. 20, pp. 4737–4740, 2000.

[60] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres et W. K. Wootters, « Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels », *Physical Review Letters*, vol. 70, no. 13, pp. 1895–1899, 1993.

[61] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter et A. Zeilinger, « Experimental quantum teleportation », *Nature*, vol. 390, pp. 575–579, 1997.

[62] D. Boschi, S. Branca, F. De Martini, L. Hardy et S. Popescu, « Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels », *Physical Review Letters*, vol. 80, no. 6, pp. 1121–1125, 1998.

[63] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden et N. Gisin, « Long-distance Teleportation of Qubits at Telecommunication Wavelengths », *Nature*, vol. 421, pp. 509–513, 2003.

[64] M. Żukowski, A. Zeilinger, M. A. Horne et A. K. Ekert, « "Event-ready-detectors" Bell experiment via entanglement swapping », *Physical Review Letters*, vol. 71, no. 26, pp. 4287–4290, 1993.

[65] J.-W. Pan, D. Bouwmeester, H. Weinfurter et A. Zeilinger, « Experimental entanglement swapping : Entangling photons that never interacted », *Physical Review Letters*, vol. 80, no. 18, pp. 3891–3894, 1998.

[66] T. Jennewein, G. Weihs, J.-W. Pan et A. Zeilinger, « Experimental nonlocality proof of quantum teleportation and entanglement swapping », *Physical Review Letters*, vol. 88, no. 1, p. 017903, 2002.

[67] H. de Riedmatten, I. Marcikic, J. A. W. van Houwelingen, W. Tittel, H. Zbinden et N. Gisin, « Long-distance entanglement swapping with photons from separated sources », *Physical Review A*, vol. 71, no. 5, p. 050302, 2005.

[68] H.-J. Briegel, W. Dür, J. I. Cirac et P. Zoller, « Quantum Repeaters : the Role of Imperfect Local Operations in Quantum Communication », *Physical Review Letters*, vol. 81, no. 26, pp. 5932–5935, 1998.

[69] K. Hammerer, A. S. Sorensen et E. S. Polzik, « Quantum interface between light and atomic ensembles ». arXiv:0807.3358, 2008.

[70] W. Tittel, M. Afzelius, T. Chanelière, R. Cone, S. Kröll, S. Moiseev et M. Sellars, « Photon-echo quantum memory in solid state systems », *Laser & Photonics Reviews*, vol. 1, pp. 1863–1883, 2009.

[71] N. Sangouard, C. Simon, H. de Riedmatten et N. Gisin, « Quantum repeaters based on atomic ensembles and linear optics ». arXiv:0906.2699, 2009.

[72] N. D. Mermin, *Quantum Computer Science : An Introduction*. Cambridge University Press, 2007.

[73] R. Feynman, « Simulating physics with computers », *International Journal of Theoretical Physics*, vol. 21, no. 6/7, pp. 467–488, 1982.

[74] D. Deutsch, « Quantum theory, the church-turing principle and the universal quantum computer », *Proceedings of the Royal Society of London A*, vol. 400, pp. 97–117, 1985.

[75] P. W. Shor, « Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer », *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[76] L. K. Grover, « Quantum mechanics helps in searching for a needle in a haystack », *Physical Review Letters*, vol. 79, no. 2, pp. 325–328, 1997.

[77] E. Knill, R. Laflamme et G. Milburn, « A scheme for efficient quantum computation with linear optics », *Nature*, vol. 409, pp. 46–52, 2001.

[78] R. Raussendorf et H. J. Briegel, « A one-way quantum computer », *Physical Review Letters*, vol. 86, no. 22, pp. 5188–5191, 2001.

[79] M. A. Nielsen, « Cluster-state quantum computation », *Reports on Mathematical Physics*, vol. 57, no. 1, pp. 147–161, 2006.

[80] P. Walther, K. J. Resch, T. E. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer et A. Zeilinger, « Experimental one-way quantum computing », *Nature*, vol. 434, pp. 169–176, 2005.

[81] R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaek, T. Jennewein et A. Zeilinger, « High-speed linear optics quantum computing using active feed-forward », *Nature*, vol. 445, pp. 65–69, 2007.

[82] G. Vallone, E. Pomarico, P. Mataloni, F. De Martini et V. Berardi, « Realization and characterization of a two-photon four-qubit linear cluster state », *Physical Review Letters*, vol. 98, no. 18, p. 180502, 2007.

[83] K. Chen, C.-M. Li, Q. Zhang, Y.-A. Chen, A. Goebel, S. Chen, A. Mair et J.-W. Pan, « Experimental realization of one-way quantum computing with two-photon four-qubit cluster states », *Physical Review Letters*, vol. 99, no. 12, p. 120503, 2007.

[84] G. Vallone, E. Pomarico, F. De Martini et P. Mataloni, « Active one-way quantum computation with two-photon four-qubit cluster states », *Physical Review Letters*, vol. 100, no. 16, p. 160502, 2008.

[85] D. E. Browne et T. Rudolph, « Resource-efficient linear optical quantum computation », *Physical Review Letters*, vol. 95, p. 010501, 2005.

[86] K. J. Resch, M. Lindenthal, B. Blauensteiner, H. R. Boehm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter et A. Zeilinger, « Distributing entanglement and single photons through an intra-city, free-space quantum channel », *Optics Express*, vol. 13, no. 1, pp. 202–209, 2005.

[87] C. Erven, C. Couteau, R. Laflamme et G. Weihs, « Entangled quantum key distribution over two free-space optical links », *Optics Express*, vol. 16, no. 21, pp. 16840–16853, 2008.

[88] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter et A. Zeilinger, « Free-space distribution of entanglement and single photons over 144 km », *Nature Physics*, vol. 3, pp. 481–486, 2007.

[89] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein et A. Zeilinger, « High-fidelity transmission of entanglement over a high-loss free-space channel », *Nature Physics*, vol. 5, pp. 389–392, 2009.

[90] P. Ciprut, B. Gisin, N. Gisin, R. Passy, P. Von Der Weld, F. Prieto et C. W. Zimmer, « Second-order polarization mode dispersion : impact on analog and digital transmissions », *Journal of Lightwave Technology*, vol. 16, no. 5, pp. 757–771, 1998.

[91] C. Liang, K. F. Lee, J. Chen et P. Kumar, « Distribution of Fiber-Generated Polarization Entangled Photon-Pairs over 100 km of Standard Fiber in OC-192 WDM Environment », *OFC 2006 Postdeadline paper PDP35*, 2006.

[92] T.-Y. Chen, J. Wang, Y. Liu, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, Z.-B. Chen et J.-W. Pan, « 200 km decoy-state quantum key distribution with photon polarization ». `arXiv:0908.4063`, 2009.

[93] H. Hübel, M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe et A. Zeilinger, « High-fidelity transmission of polarization encoded qu-

bits from an entangled source over 100 km of fiber », *Optics Express*, vol. 15, no. 12, pp. 7853–7862, 2007.

[94] C. H. Bennett, « Quantum cryptography using any two nonorthogonal states », *Physical Review Letters*, vol. 68, no. 21, pp. 3121–3124, 1992.

[95] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré et N. Gisin, « Distribution of Time-Bin Entangled Qubits over 50 km of Optical Fiber », *Physical Review Letters*, vol. 93, p. 180502, 2004.

[96] S.Fasel, N.Gisin, G.Ribordy et H.Zbinden, « Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs : a comparison of two chromatic dispersion reduction methods », *The European Physical Journal D*, vol. 30, no. 1, pp. 143–148, 2004.

[97] H. Takesue, « Long-distance distribution of time-bin entanglement generated in a cooled fiber », *Optics Express*, vol. 14, no. 8, pp. 3453–3460, 2006.

[98] I. L. Chuang et Y. Yamamoto, « Simple quantum computer », *Physical Review A*, vol. 52, pp. 3489–3496, 1995.

[99] P. C. Sun, Y. Mazurenko et Y. Fainman, « Long-distance frequency-division interferometer for communication and quantum cryptography », *Optics Letters*, vol. 20, no. 9, pp. 1062–1063, 1995.

[100] Y. T. Mazurenko, R. Giust et J. P. Goedgebuer, « Spectral coding for secure optical communications using refractive index dispersion », *Optics Communications*, vol. 133, pp. 87–92, 1997.

[101] J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer et W. T. Rhodes, « Single-photon interference in sidebands of phase-modulated light for quantum cryptography », *Physical Review Letters*, vol. 82, no. 8, pp. 1656–1659, 1999.

[102] A. Mair, A. Vaziri, G. Weihs et A. Zeilinger, « Entanglement of the orbital angular momentum states of photons », *Nature*, vol. 412, pp. 313–316, 2001.

[103] H. C. Lefevre, « Single-mode fibre fractional wave devices and polarisation controllers », *Electronics Letters*, vol. 16, no. 20, pp. 778–780, 1980.

[104] N. J. Cerf, M. Bourennane, A. Karlsson et N. Gisin, « Security of Quantum Key Distribution Using d-Level Systems », *Physical Review Letters*, vol. 88, no. 12, p. 127902, 2002.

[105] M. Fujiwara, M. Takeoka, J. Mizuno et M. Sasaki, « Exceeding the Classical Capacity Limit in a Quantum Optical Channel », *Physical Review Letters*, vol. 90, no. 16, p. 167906, 2003.

[106] Č. Brukner, M. Żukowski et A. Zeilinger, « Quantum Communication Complexity Protocol with Two Entangled Qutrits », *Physical Review Letters*, vol. 89, no. 19, p. 197901, 2002.

[107] M. Fitzi, N. Gisin et U. Maurer, « Quantum Solution to the Byzantine Agreement Problem », *Physical Review Letters*, vol. 87, no. 21, p. 217901, 2001.

[108] M. Barbieri, F. De Martini, P. Mataloni, G. Vallone et A. Cabello, « Enhancing the violation of the Einstein-Podolsky-Rosen local realism by quantum hyperentanglement », *Physical Review Letters*, vol. 97, p. 140407, 2006.

[109] D. Collins, N. Gisin, N. Linden, S. Massar et S. Popescu, « Bell Inequalities for Arbitrarily High-Dimensional Systems », *Physical Review Letters*, vol. 88, no. 4, p. 040404, 2002.

[110] M. Reck, A. Zeilinger, H. J. Bernstein et P. Bertani, « Experimental Realization of Any Discrete Unitary Operator », *Physical Review Letters*, vol. 73, no. 1, pp. 58–61, 1994.

[111] H. Bechmann-Pasquinucci et A. Peres, « Quantum Cryptography with 3-State Systems », *Physical Review Letters*, vol. 85, no. 15, pp. 3313–3316, 2000.

[112] A. N. Zhang, C. Y. Lu, X. Q. Zhou, Y. A. Chen, Z. Zhao, T. Yang et J. W. Pan, « Experimental construction of optical multiqubit cluster states from Bell states », *Physical Review A*, vol. 73, p. 022330, 2006.

[113] Y. Soudagar, F. Bussières, G. Berlín, S. Lacroix, J. M. Fernandez et N. Godbout, « Cluster state quantum computing in optical fibers », *Journal of the Optical Society of America B*, vol. 24, no. 2, pp. 226–230, 2006.

[114] R. W. Boyd, *Nonlinear Optics*. Academic Press, 3e éd., 2002.

[115] E. S. Fry et R. C. Thompson, « Experimental test of local hidden-variable theories », *Physical Review Letters*, vol. 37, no. 8, pp. 465–468, 1976.

[116] C. K. Hong, Z. Y. Ou et L. Mandel, « Measurement of subpicosecond time intervals between two photons by interference », *Physical Review Letters*, vol. 59, no. 18, pp. 2044–2046, 1987.

[117] Z. Y. Ou, C. K. Hong et L. Mandel, « Violations of locality in correlation measurements with a beam splitter », *Physics Letters A*, vol. 122, no. 1, pp. 11–13, 1987.

[118] Z. Y. Ou et L. Mandel, « Violation of Bell's inequality and classical probability in a two-photon correlation experiment », *Physical Review Letters*, vol. 61, no. 1, pp. 50–53, 1988.

[119] L. Mandel et E. Wolf, *Optical coherence and quantum optics*. Cambridge University Press, 1995.

[120] D. C. Burnham et D. L. Weinberg, « Observation of simultaneity in parametric production of optical photon pairs », *Physical Review Letters*, vol. 25, no. 2, pp. 84–87, 1970.

[121] D. H. Jundt, « Temperature-dependent Sellmeier equation for the index of refraction, n_e, in congruent lithium niobate », *Optics Express*, vol. 22, no. 20, pp. 1553–1555, 1997.

[122] C. C. Gerry et P. L. Knight, *Introductory Quantum Optics*. Cambridge University Press, 2005.

[123] H. D. Riedmatten, V. Scarani, I. Marcikic, A. Acín, W. Tittel, H. Zbinden et N. Gisin, « Two independent photon pairs versus four-photon entangled states in parametric down conversion », *Journal of Modern Optics*, vol. 15, no. 11, pp. 1637–1649, 2004.

[124] M. Fiorentino, P. L. Voss, J. E. Sharping et P. Kumar, « All-fiber photon-pair source for quantum communications », *IEEE Photonics Technology Letters*, vol. 14, no. 7, pp. 983–985, 2002.

[125] L.-M. Duan, M. D. Lukin, J. I. Cirac et P. Zoller, « Long-distance quantum communication with atomic ensembles and linear optics », *Nature*, vol. 414, pp. 413–418, 2001.

[126] A. Kuzmich, W. P. Bowen, A. D. Boozer, A. Boca, C. W. Chou, L.-M. Duan et H. J. Kimble, « Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles », *Nature*, vol. 423, pp. 731–734, 2003.

[127] T. Chanelière, D. N. Matsukevich, S. D. Jenkins, T. A. B. Kennedy, M. S. Chapman et A. Kuzmich, « Quantum telecommunication based on atomic cascade transitions », *Physical Review Letters*, vol. 96, no. 9, p. 093604, 2006.

[128] J. Simon, H. Tanji, J. K. Thompson et V. Vuletic, « Interfacing collective atomic excitations and single photons », *Physical Review Letters*, vol. 98, no. 18, p. 183601, 2007.

[129] R. Hanbury Brown et R. Q. Twiss, « Correlation between photons in two coherent beams of light », *Nature*, vol. 177, pp. 27–29, 1956.

[130] P. Grangier, G. Roger et A. Aspect, « Experimental evidence for a photon anticorrelation effect on a beam splitter : A new light on single-photon interferences », *Europhysics Letters*, vol. 1, no. 4, pp. 173–179, 1986.

[131] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres et W. K. Wootters, « Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels », *Physical Review Letters*, vol. 70, no. 13, pp. 1895–1899, 1993.

[132] C. K. Hong et L. Mandel, « Experimental realization of a localized one-photon state », *Physical Review Letters*, vol. 56, no. 1, pp. 58–60, 1986.

[133] X. Ma, C.-H. Fred Fung et H.-K. Lo, « Quantum key distribution with entangled photon sources », *Physical Review A*, vol. 76, no. 1, p. 012307, 2007.

[134] E. Waks, C. Santori et Y. Yamamoto, « Security aspects of quantum key distribution with sub-Poisson light », *Physical Review A*, vol. 66, no. 4, p. 042315, 2002.

[135] Q. W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo et A. Karlsson, « Experimental decoy-state quantum key distribution with a sub-Poissionian heralded single-photon source », *Physical Review Letters*, vol. 100, no. 9, p. 090501, 2008.

[136] Y. Adachi, T. Yamamoto, M. Koashi et N. Imoto, « Simple and efficient quantum key distribution with parametric down-conversion », *Physical Review Letters*, vol. 99, no. 18, p. 180503, 2007.

[137] W. Mauerer et C. Silberhorn, « Quantum key distribution with passive decoy state selection », *Physical Review A*, vol. 75, no. 5, p. 050305, 2007.

[138] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden et N. Gisin, « Quantum interference with photon pairs created in spatially separated sources », *Physical Review A*, vol. 67, no. 2, p. 022301, 2003.

[139] S. Takeuchi, R. Okamoto et K. Sasaki, « High-yield single-photon source using gated spontaneous parametric downconversion », *Applied Optics*, vol. 43, no. 30, pp. 5708–5711, 2004.

[140] R. Okamoto, S. Takeuchi et K. Sasaki, « Detailed analysis of a single-photon source using gated spontaneous parametric downconversion », *Journal of the Optical Society of America B*, vol. 22, no. 11, pp. 2393–2401, 2005.

[141] M. Tengner et D. Ljunggren, « Characterization of an asynchronous source of heralded single photons generated at a wavelength of 1550 nm ». `arXiv:0706.2985`, 2007.

[142] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden et N. Gisin, « Time-bin entangled qubits for quantum communication created by femtosecond pulses », *Physical Review A*, vol. 66, no. 6, p. 062308, 2002.

[143] F. Bussières, *Cryptographie quantique à plusieurs participants par multiplexage en longueur d'onde*. Mémoire de maîtrise, Université de Montréal, 2003.

[144] J. D. Franson, « Nonlocal cancellation of dispersion », *Physical Review A*, vol. 45, no. 5, pp. 3126–3132, 1992.

[145] P. J. Mosley, J. S. Lundeen, B. J. Smith, P. Wasylczyk, A. B. U'Ren, C. Silberhorn et I. A. Walmsley, « Heralded generation of ultrafast single photons in pure quantum states », *Physical Review Letters*, vol. 100, no. 13, p. 133601, 2008.

[146] J. A. Slater, J.-S. Corbeil, S. Virally, F. Bussisères, A. Kudlinski, G. Bouwmans, S. Lacroix, N. Godbout et W. Tittel, « A microstructured fiber source of photon pairs at widely separated wavelengths ». `arXiv:0908.3516`, 2009.

[147] C. E. Kuklewicz, M. Fiorentino, G. Messin, F. N. C. Wong et J. H. Shapiro, « High-flux source of polarization-entangled photons from a periodically poled $KTiOPO_4$ parametric down-converter », *Physical Review A*, vol. 69, no. 1, p. 013807, 2004.

[148] X. Li, P. L. Voss, J. E. Sharping et P. Kumar, « Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band », *Physical Review Letters*, vol. 94, no. 5, p. 053601, 2005.

[149] J. Fulconis, O. Alibart, J. L. O'Brien, W. J. Wadsworth et J. G. Rarity, « Nonclassical interference and entanglement generation using a photonic crystal fiber pair photon source », *Physical Review Letters*, vol. 99, no. 12, p. 120501, 2007.

[150] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden et N. Gisin, « Experimental investigation of the robustness of partially entangled qubits over 11 km », *Physical Review A*, vol. 66, no. 6, p. 062304, 2002.

[151] J. M. Raimond, M. Brune et S. Haroche, « Manipulating quantum entanglement with atoms and photons in a cavity », *Reviews of Modern Physics*, vol. 73, no. 3, pp. 565–582, 2001.

[152] S. Sauge, M. Swillo, M. Tengner et A. Karlsson, « A single-crystal source of path-polarization entangled photons at non-degenerate wavelengths », *Optics Express*, vol. 16, pp. 9701–9707, 2008.

[153] X.-s. Ma, A. Qarry, J. Kofler, T. Jennewein et A. Zeilinger, « Experimental violation of a Bell inequality with two different degrees of freedom of entangled particle pairs », *Physical Review A*, vol. 79, no. 4, p. 042101, 2009.

[154] F. Bussières, N. Godbout et W. Tittel, « Hybrid entanglement for optical quantum networks », *38th Annual Meeting of the Division of Atomic, Molecular, and Optical Physics, Calgary, Alberta, Canada*, 2007.

[155] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb et A. Zeilinger, « Long-distance quantum communication with entangled photons using satellites », *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 9, no. 6, pp. 1541–1551, 2003.

[156] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*. Cambridge University Press, 1987.

[157] B. S. Cirel'son, « Quantum generalizations of Bell's inequality », *Letters in Mathematical Physics*, vol. 4, no. 2, pp. 93–100, 1980.

[158] A. Peres, « Separability criterion for density matrices », *Physical Review Letters*, vol. 77, no. 8, pp. 1413–1415, 1996.

[159] J. F. Clauser et M. A. Horne, « Experimental consequences of objective local theories », *Physical Review D*, vol. 10, no. 2, pp. 526–535, 1974.

[160] W. Tittel, J. Brendel, N. Gisin et H. Zbinden, « Long-distance Bell-type tests using energy-time entangled photons », *Physical Review A*, vol. 59, pp. 4150–4163, June 1999.

[161] D. Mayers, « Unconditional security in quantum cryptography », *Journal of the ACM*, vol. 48, no. 3, pp. 351–406, 2001.

[162] P. W. Shor et J. Preskill, « Simple proof of security of the BB84 quantum key distribution protocol », *Physical Review Letters*, vol. 85, no. 2, pp. 441–444, 2000.

[163] P. M. Pearle, « Hidden-variable example based upon data rejection », *Physical Review D*, vol. 2, no. 8, pp. 1418–1425, 1970.

[164] A. Garg et N. D. Mermin, « Detector inefficiencies in the Einstein-Podolsky-Rosen experiment », *Physical Review D*, vol. 35, no. 12, pp. 3831–3835, 1987.

[165] P. H. Eberhard, « Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment », *Physical Review A*, vol. 47, no. 2, pp. R747–R750, 1993.

[166] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe et D. J. Wineland, « Experimental violation of a Bell's inequality with efficient detection », *Nature*, vol. 409, pp. 791–794, 2000.

[167] T. Paterek, A. Fedrizzi, S. Gröblacher, T. Jennewein, M. Żukowski, M. Aspelmeyer et A. Zeilinger, « Experimental test of nonlocal realistic theories without the rotational symmetry assumption », *Physical Review Letters*, vol. 99, no. 21, p. 210406, 2007.

[168] C. Branciard, A. Ling, N. Gisin, C. Kurtsiefer, A. Lamas-Linares et V. Scarani, « Experimental falsification of Leggett's nonlocal variable model », *Physical Review Letters*, vol. 99, no. 21, p. 210407, 2007.

[169] S. Gröblacher, T. Paterek, R. Kaltenbaek, Č. Brukner, M. Żukowski, M. Aspelmeyer et A. Zeilinger, « An experimental test of non-local realism », *Nature*, vol. 446, pp. 871–875, 2007.

[170] N. Gisin, « Bell inequalities : many questions, a few answers ». `arXiv:quant-ph/0702021`, 2007.

[171] I. L. Martinez, P. Chan, X. Mo, S. Hosier et W. Tittel, « Proof-of-concept of real-world quantum key distribution with quantum frames », *New Journal of Physics*, vol. 11, p. 095011, 2009.

[172] J. A. Slater, « Photon pair technologies for quantum communication », Mémoire de maîtrise, University of Calgary, 2009.

[173] A. Kent, « Coin tossing is strictly weaker than bit commitment », *Physical Review Letters*, vol. 83, no. 25, pp. 5382–5384, 1999.

[174] D. Aharonov, A. Ta-Shma, U. Vazirani et A. C.-C. Yao, « Quantum bit escrow », *Proceedings of 32nd Annual ACM Symposium on Theory of Computing, Portland, Oregon, USA*, pp. 705–714, 2000.

[175] R. W. Spekkens et T. Rudolph, « Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol », *Quantum Information and Computation*, vol. 2, no. 1, pp. 66–96, 2002.

[176] R. W. Spekkens et T. Rudolph, « Degrees of concealment and bindingness in quantum bit commitment protocols », *Physical Review A*, vol. 65, no. 1, p. 012310, 2001.

[177] A. Ambainis, « A new protocol and lower bounds for quantum coin flipping », *Journal of Computer and System Sciences*, vol. 68, no. 2, pp. 398–416, 2004.

[178] A. Chailloux et I. Kerenidis, « Optimal quantum strong coin flipping ». `arXiv:0904.1511`, 2009.

[179] H. Buhrman, M. Christandl, M. Koucký, Z. Lotker, B. Patt-Shamir et N. K. Vereshchagin, « High entropy random selection protocols », *Proceedings of 11th International Workshop on Randomization and Computation (RANDOM 2007), Princeton, NJ, USA*, pp. 366–379, 2007.

[180] A. T. Nguyen, J. Frison, K. Phan Huy et S. Massar, « Experimental quantum tossing of a single coin », *New Journal of Physics*, vol. 10, p. 083037, 2008.

[181] G. Berlín, G. Brassard, F. Bussières et N. Godbout, « Fair loss-tolerant quantum coin flipping », *Physical Review A (à paraître)*, 2009.

[182] D. Mayers, « Unconditionally secure quantum bit commitment is impossible », *Physical Review Letters*, vol. 78, no. 17, pp. 3414–3417, 1997.

[183] H.-K. Lo et H. F. Chau, « Is quantum bit commitment really possible ? », *Physical Review Letters*, vol. 78, no. 17, pp. 3410–3413, 1997.

[184] C. W. Helstrom, *Quantum Detection and Estimation Theory*. Academic Press, New York, 1976.

[185] C. A. Fuchs et J. van de Graaf, « Cryptographic distinguishability measures for quantum-mechanical states », *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1216–1227, 1999.

[186] T. Rudolph, R. W. Spekkens et P. S. Turner, « Unambiguous discrimination of mixed states », *Physical Review A*, vol. 68, no. 1, p. 010301, 2003.

[187] I. D. Ivanovic, « How to differentiate between non-orthogonal states », *Physics Letters A*, vol. 123, no. 6, pp. 257–259, 1987.

[188] D. Dieks, « Overlap and distinguishability of quantum states », *Physics Letters A*, vol. 126, no. 5-6, pp. 303–306, 1988.

[189] A. Peres, « How to differentiate between non-orthogonal states », *Physics Letters A*, vol. 128, no. 1, p. 19, 1988.

[190] A. Chefles et S. M. Barnett, « Strategies for discriminating between non-orthogonal quantum states », *Journal of Modern Optics*, vol. 45, no. 6, pp. 1295–1302, 1998.

[191] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson et J. Jeffers, « Maximum confidence quantum measurements », *Physical Review Letters*, vol. 96, no. 7, p. 070401, 2006.

[192] C. Mochon, « Quantum weak coin flipping with arbitrarily small bias ». `arXiv:0711.4114`, 2007.

[193] R. W. Spekkens et T. Rudolph, « Quantum protocol for cheat-sensitive weak coin flipping », *Physical Review Letters*, vol. 89, no. 22, p. 227901, 2002.

[194] G. Molina-Terriza, A. Vaziri, R. Ursin et A. Zeilinger, « Experimental quantum coin tossing », *Physical Review Letters*, vol. 94, no. 4, p. 040501, 2005.